Algebraic Number Theory

Winter Term 2020/21

Lecture by Christopher Deninger
Notes taken by Florian Riedel

February 18, 2021

Contents

1 Integrality **3**

2 Dedekind Rings **10**

3 Minkowski Theory **16**

4 Decomposition Laws **30**

5 Decomposition Laws in Quadratic Fields **39**

6 Quadratic reciprocity **40**

7 Hilbert Theory **41**

8 Decomposition of primes in cyclotomic fields **46**

1 Integrality

Aim: Want to define Integral closures of algebraic extensions of $\mathbb{Q}$.
All rings will be unital and commutative and ring maps preserve the unit.

Definition 1.1. $A \subseteq B$ a extension of rings. We call $b \in B$ *integral* over A if there exists a monic polynomial $p \in A[T]$ such that $p(b) = 0$. We say that B is *integral* over A if every element of B is.

Theorem 1.2. *Elements $b_1, \ldots, b_k \in B$ are integral over A iff the subring $A[b_1, \ldots, b_k] \subseteq B$ is finitely generated as an A-Module.*

Proof. Assume $b \in B$ integral over A, and $p \in A[T]$ such that b is a root. Then $p(b) = 0$ implies that b^i for $i \geq n$ is and A-linear combination of $\{1, b^1, \ldots, b^{n-1}\}$ for $n = \deg(p)$. Hence $A[b]$ is finitely generated as an A-module. The general case follows inductively. This proves the "only if" part.
For the "if" part assume that $A[b_i]$ is a finitely generated A-module with generators $w_1, \ldots, W_m$. Then for $b \in A[b_i]$ we have:

$$bw_i = \sum_j a_{ij} w_j \quad \text{for some } a_{ij} \in A$$

Recall that for every M a $m \times m$ matrix we have the Laplace formula:

$$MM^* = M^*M = \det(M) \operatorname{id}_m$$

Where $M^*_{ij} = (-1)^{i+j} \det(M_{ij})$ and M_{ij} is M with the i-th row and j-th column deleted. Now set $M = b \operatorname{id}_m - (a_{ij})$ and $w = (w_i)$. Then our equation becomes simply:

$$Mw = 0$$

Applying Laplace we get that (M)$w_i = 0$. Since $1 \in A[b_i]$ is an A-linear combination of the w_i we have that $\det(M) = 0$ i.e.:

$$\det(b \operatorname{id}_m - (a_{ij}))$$

This is a monic polynomial equation over A for b. Hence b is integral over A. □

Corollary 1.3.

- *$A \subset B$ a ring extension. Define:*

$$A^{\sim} := \{b \in B \mid b \text{ is integral over } A\}$$

  Then $A \subset A^{\sim} \subset B$ is a subring of B called the integral closure of A in B

- *$A \subset B \subset C$ ring extensions. If C/B and B/A are integral then C/A is integral.*

Definition 1.4.

- For $A \subset B$ we say that A is integrally closed in B if we have $A^{\sim} = A$
- If A is a domain is called integrally closed if it is in its fraction field.

Remark 1.5.

- Integral closures are integrally closed
- Every factorial ring and hence every principal ideal domain A is integrally closed. [Indeed: Let $x \in K = \operatorname{Quot}(A)$ satisfying $p(x) = 0$ with $p = a_N J^n + \ldots a_0$. Write $x = a/b$ with $a, b \in A$ coprime. Then:

$$a^n + a_{n-1} b a^{n-1} + \ldots a_0 b^n = 0$$

  Assume some prime element π divides b, then π divides a^n and consequently also a. Thus there is no such π and thus b is a unit.]

Now lets turn to the most important example for us: Let $K/\mathbb{Q}$ be algebraic and $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K. Then we've seen that $\mathcal{O}_K$ is an integrally closed subring of K.
The transitive property of integrality implies that for algebraic extensions:

$$\mathbb{Q} \subset K \subset L$$

The ring $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.
Question: How can we efficiently check integrality of an element?

Proposition 1.6. *Let A be an integrally closed domain with quotient field K. Let L/K be and algebraic extension. For $\beta \in L$ let $p \in K[T]$ be the minimal polynomial of β over K. Then: β is integral over A iff $p \in A[X]$*

Proof. The "if" part is clear since p is monic. For the "only if part" let $q \in A[T]$ be a monic polynomial with $q(\beta) = 0$. Choose a finite extension $L^{\sim}/L$ such that q decomposes into linear factors in $L^{\sim}$. Since p divides q in $K[t] \subset L^{\sim}[T]$, also p decomposes into linear factors in $L^{\sim}[T]$, and the roots of p in $L^{\sim}$ are integral over A (Since they are roots of q). Hence the coefficients c_i of p are integral over A. Since $c_i \in K$ we in fact must have $c_i \in A$ since A is integrally closed. □

Corollary 1.7. *Let $K/\mathbb{Q}$ be a quadratic field. Then there exists a squarefree $d \in \mathbb{Z}$ with $d \neq 1$ and $K = \mathbb{Q}(\sqrt{d})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if $d - 1$ is not divisible by 4. Otherwise we have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.*

Proof. For $d - 1$ not divisible by 4 respectively $d - 1$ divisible by 4 the minimal polynomials with coefficients in $\mathbb{Z}$ are

$$X^2 - d \text{ resp. } X^2 - X + \frac{1-d}{4}$$

Have zeroes $\sqrt{d}$ resp. $\frac{1+\sqrt{d}}{2}$. Hence these elements are integral over $\mathbb{Z}$ and thus lie in $\mathcal{O}_K$. This proves the one inclusion. For the other one let $a \in \mathcal{O}_K$ with minimal polynomial $P(X)$. Then $P \in \mathbb{Z}[X]$.

- $a \in \mathbb{Q}$ then $P(X) = X - a$, hence $a \in \mathbb{Z} \subset$ rhs
- a not in $\mathbb{Q}$, then $a =$ $frac\alpha + \beta\sqrt{d}2$ $\alpha, \beta \in \mathbb{Q}$ with $\beta \neq 0$. Setting $a' := \frac{\alpha - \beta\sqrt{d}}{2}$ we have

  $$P(X) = (X - a)(X - a)' = X^2 - \alpha + frac\alpha^2 - d\beta^2 4)$$

  Hence $\alpha \in \mathbb{Z}$ and $\alpha^2 - d\beta^2 \in 4\mathbb{Z}$. Hence $d\beta^2 \in \mathbb{Z}$. Thus $\beta \in \mathbb{Z}$ since d was by assumption square free.
  If d is not $1 \mod 4$ then since d is not $0 \mod$ have that

  $$d \cong 2, 3 \mod 4$$

  On the other hand $\alpha^2, \beta^2 \cong 0, 1 \mod 4$. We know that $\alpha^2 \equiv d\beta^2 \mod 4$. This implies

  $$\alpha^2, \beta^2 \equiv \mod 4 \implies 2|\alpha, \beta$$

  and consequently $a \in \mathbb{Z}[\sqrt{d}]$
  For $d \equiv 1 \mod 4$ we get

  $$0 \equiv \alpha^2 - d\beta^2 \equiv \alpha^2 - \beta^2 \equiv (\alpha - \beta)(\alpha + \beta) \mod 4$$

  Thus $2|\alpha - \beta$ or $2|\alpha - \beta$, but $\alpha - \beta = (\alpha + \beta - 2\beta$ hence $2|\alpha - \beta$

□

Notation: Let L/K be a finite field extensions. For $x \in L$ consider the K-linear map

$$m_x : L \to L \quad y \mapsto xy$$

. Set $\mathrm{Tr}_{L/K}(x) := \mathrm{Tr}(m_x)$
and $N_{L/K}(x) := \det(m_x) \in K$
Then $\mathrm{Tr} : L \to K$ is additive and $N : L^\times \to K^\times$ is multiplicative. Since the map $L \to \mathrm{Hom}_K(L, L)$ is a ring morphism. The trace and norm are coefficients of the characteristic polynomial of m_x:

$$P_{m_x} := \det(t\,\mathrm{id} - m_x) = t^n - \mathrm{Tr}(m_x) + \cdots + (-1)^n N(x)$$

For $n = \deg(L/K)$.

Theorem 1.8. *If L/K is a finite separable extension and if $\sigma : L \to \bar{K}$ runs over the $n = \deg(L/K)$ pairwise different embeddings of L into the algebraic closure of K. Then we have for all $x \in L$:*

$$P_{m_x} = \prod_\sigma (t - \sigma(x))$$

In particular :

$$\mathrm{Tr}_{L/K}(x) = \sum_\sigma \sigma(x)$$

$$N_{L/K}(x) = \prod_\sigma \sigma(x)$$

Proof. Let $m_x(t)$ be the minimal polynomial of x over K.If $r = \deg(K(x)/K)$, then

$$m_x(t) = t^r - c_{r-1}t^{r-1} - \dots c_0 \qquad c_i \in K$$

Claim: $P_{m_x} = m_x^d$ where $d = \deg(L/K(x)) = m/r$
Proof of Claim: Consider the basis $1, x, \dots, x^{r-1}$ of $K(x)/K$ and choose a basis $a_1, \dots, a_d$ f $L/K(x)$. Then:

$$a_1, a_1x, \dots a_1x^{r-1}, \dots, a_dx, \dots, a_dx^{r-1}$$

is a K-basis of L. In this basis the matrix of m_x is a dxd block matrix with copies of A along the diagonal where A has 1's on the off diagonal and 0 else except the last line which consists of $c_1, /dotsc_{r-1}$(The "almost Jordan Form"). Then:

$$det(t\,\mathrm{id} - A) = t^r - c_{r-1}t^{r-1} - \cdots - c_0 = m_x(t)$$

Hence $P_{m_x}(r) = det(t\,\mathrm{id} - A)^d = m_x(t)^d$ which implies our first claim.
For $\sigma, \tau in \,\mathrm{Hom}_K(L, \bar{K})$ say $\sigma \sim \tau$ if they agree on $x \in K$. Choose a system of representatives $\sigma_1, \dots \sigma_r$ for this relation. Then:

$$\mathrm{Hom}_K(K(x), \bar{K}) = \{\sigma_r|_{K(x)}, \dots \sigma_r|_{K(x)}\}$$

and:

$$m_x(t) := \prod_i (t - \sigma_i(x))$$

Indeed: both sides are monic polynomials of the same degree r with the same zeroes $\sigma_i(x)$ and are thus equal. Now we know by our earlier claim:

$$P_{m_x}(t) = m_x(t)^d = \prod_i (t - \sigma(x))^d = \prod_i \prod_{\sigma \sim \sigma_i} (t - \sigma(x)) = \prod_\sigma (t - \sigma(x))$$

Were we have used that separability implies that for each σ_i there are exactly d equivalent σ's (i.e. the extensions of $\sigma_i|_{K(x)}$ to L). ☐

Corollary 1.9. *For finite field extensions $K \subset L \subset M$ we have that:*

$$TrL/K \circ Tr_{M/L} = Tr_{M/K}$$

and

$$N_{L/K} \circ N_{M/L} = N_{M/K}$$

Proof. We only prove the case M/K separable but it is true in general.
The set $\mathrm{Hom}_K(M, \bar{K})$ decomposes in $n = \deg(L/K)$ equivalence relations under :

$$sigma \sim \tau \iff \sigma|_L = \tau|_L$$

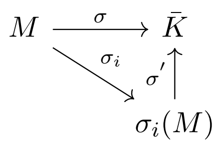
Namely given n representatives σ_i the:

$$\mathrm{Hom}_K(L, \bar{K}) = \{\sigma_i|_L \quad i\}$$

Hnece for $x \in M$ we can write:

$$Tr_{M/K}(x) = \sum_i \sum_{\sigma \sim \sigma_i} \sigma(x) = \sum_i Tr_{\sigma_i(M)/\sigma_i(L)}(\sigma_i(x))$$

[For the rightmost equation consider:



The σ's with $\sigma \sim \sigma_i$ correspond to the σ' with $\sigma'|_{\sigma_i(L)} = \mathrm{id}$. Now use Thm1.4. for $\sigma_i(M)/\sigma_i(L)$.
Note: $\sigma = \sigma' \circ \sigma_i$] Get

$$Tr_{M/K}(x) = \sum_i \sigma_i(Tr_{M/L}(x)) = Tr_{L/K} \circ Tr_{M/L}(x)$$

And a similiar argument for the norm. □

Final notation:

Definition 1.10. L/K finite separable field extension with $a_1, \dots, a_n$ a K-basis of L. Set:

$$d(a_1, \dots, a_n) := \det(A)^2$$

Where $A = (\sigma_i(a_j))_{i,j}$ and $\mathrm{Hom}_K(L, \bar{K} = \{\sigma_1, \dots, \sigma_n\})$. This element is called the *discriminant* of $a_1, \dots, a_n$. It is clearly invariant under permutation of the σ_i and α_j

Alternatively:

$$Tr_{L/K}(a_i a_j) = \sum_k \sigma_k(a_i a_j) = \sum_k \sigma_k(a_i)\sigma_k(a_j)$$

implies that:

$$(Tr_{L/K}(a_i a_j)_{i,j}) = A^t A$$

In particular we have $d(a_1, \dots, a_n) = \det((Tr_{L/K}(a_i a_j)_{ij}) \in K$. Example:
If some element $x \in \bar{K}$ is separable over K and if $n = \deg(K(x)/K)$ then the basis $\{1, x, \dots, x^{-1}\}$ of $L = K(x)$ has discriminant (Vandermonde determinant)

$$d(x, \dots, x^{n-1}) = \prod_{i<j}(x_i - x_j)^2 = \prod_{i<j}(\sigma_i(x) - \sigma_j(x))^2$$

where $x_i = \sigma_i(x)$. Exercise: the rhs is equal to:

$$\pm N_{K/\mathbb{Q}}(f^{'}(x))$$

Where f is the minimal polynomial of x.
In particular we see that the the discriminant is nonzero since by separability $x_i \neq x_j$. Now for a first application of the discriminant

Corollary 1.11. *For L/K finite separable the K-bilinear form:*

$$(-,-) : L \times L \to K, \quad (x,y) \mapsto Tr_{L/K}(xy)$$

is non-degenerate. Furthermore if $a_1, \dots, a_n$ is a basis of L over K then:

$$d(a_1, \dots, a_n) \neq 0$$

Remark 1.12. Since this is a perfect pairing it induces a K-linear isomorphism $L \xrightarrow{\sim} L^\vee$.

Proof. Since L/K is finite separable there exists a $\theta \in L$ such that $L = K(\theta)$. In terms of the basis $\{1, \theta, \dots, \theta^{n-1}\}$ the matrix M of the form $(-,-)$ is given by:

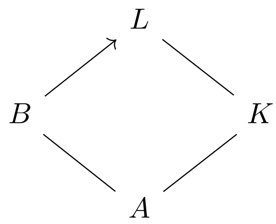
$$M = (Tr_{L/K}(\theta^{i-1}\theta^{j-1}))_{i,j}$$

And thus:

$$\det M = d(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j} (\sigma_i(\theta - \sigma_j(\theta))^2 \neq 0$$

Hence M is invertible and the pairing is perfect. In particular the matrix N with respect to the basis $a_1, \dots, a_n$ is invertible as well but by doing the same logic backwards we see that $d(a_1, \dots, a_n) \neq 0$ as claimed. $\square$

Proposition 1.13. *Let A be an integrally closed domain with quotient field K and let B be the integral closure of A in a finite separable field extension L/K.*



(1)

Then:

- *For $x \in B$ we have $Tr_{L/K}(x) \in A$ and $N_{L/K}(x) \in A$*
- *For $x \in B$ we have that $x \in B^\times \iff N_{L/K}(x) \in A^\times$*

Proof.
- $x \in B \implies x^m + a_{m-1}x^{m-1} + \dots a_o = 0$ For $a_i \in A$. for $\sigma \in \mathrm{Hom}_K(L, \bar{K})$ we get:

$$\sigma(x)^m + a_{m-1}\sigma(x)^{n-1} + \dots + a_0$$

and hence $\sigma(x) \in \bar{K}$ is integral over A and consequently:

$$Tr_{L/K}(x) = \sum_\sigma \sigma(x)$$

is integral over A. Since $Tr_{L/K} \in K$ and since A is integrally closed in K we see that $Tr_{L/K}(x) \in A$. Same argument works for the norm.

– $x \in B^\times \implies xy = 1$ for some $y \in B$ hence:

$$N_{L/K}(x)N_{L/K}(y) = 1$$

Since both factors are in A we get that $N_{L/K}(x) \in A^\times$. Now consider some $x \in B$ with $N_{L/K}(x) \in A^\times$. Then there exists some $a \in A$ with:

$$1 = aN_{L/K}(x) = a\prod_{\sigma} \sigma(x) = (a \prod_{\sigma \neq \mathrm{id}} \sigma(x))x$$

Here we view L as a subfield of $\bar{K}$ and denote the corresponding embedding by id. So the element:

$$y := a \prod_{\sigma \neq \mathrm{id}} \sigma(x) = x^{-1} \in L$$

is integral over A (since the a and the $\sigma(x)$ are) and hence lies in B.

□

Now we give an estimate for the denominators of elements in B:

Theorem 1.14. *In the situation of the previous proposition let $w_1, \dots, w_n \in B$ be a basis of L/K with discriminant $d = d(w_1, \dots, w_n)$ then:*

$$dB \subseteq Aw_1 + \dots Aw_n$$

Remark 1.15. For $x \in L$ there exists some $0 \neq a \in A$ with $ax \in B$

Proof. Since L/K there exists an equation:

$$x^n c_{n-1}x^{n-1} + \dots + c_0 = 0$$

with $c_i \in K$. Since K is the quotient field of A there exists some $0 \neq a \in A$ with $ac_i \in A$ for all i. Multiplying the equation by a^n the gives an equation for ax with coefficients in A:

$$(ax)^n + ac_{n-1}(ax)^{n-1} + \dots + a^n c_0 = 0$$

And thus $ax \in L$ is integral over A, hence lies in B. □

Consequences:

– A basis as in the theorem always exists.

– Quot$B = L$

Proof. Fir $w \in B$ there exits $x_j \in K$ such that:

$$w = \sum_{j=1}^{n} x_j w_j$$

Hence we get by applying the trace:

$$Tr_{L/K}(w_i w) = \sum_{j=1}^{n} x_j Tr_{L/K}(w_i w_j) \tag{2}$$

Since $0 \neq d = \det(Tr_{L/K}(w_i w_j))$ by assumption this has a unique solution. Specifically Cramer's rule gives:

$$x_j = \frac{a_j}{d} \text{ for certain } a_j \in A$$

So we get:

$$dw = \sum_{j=1}^{n} (dx_j)w_j = \sum_{j=1}^{n} a_j w_j \in Aw_1 + \dots + Aw_n$$

□

Definition 1.16. In the situation of prop(ref) assume that B is a free A-module of rank n. Then a basis $w_1, \dots, w_n \in B$ over A is called an *integral basis* of B over A. Such a basis is easily seen to be a basis of L/K as well and thus:

$$n = \text{rnk}_A\, B = \deg(L/B)$$

Remark 1.17. In general B is not free as an A-module, so integral bases may not exist.

Theorem 1.18. *Assume that in the Situation of our proposition the ring A is a PID. Then B and more generally every finitely generated B-submodule $M \neq 0$ of L is free of rank $n = \deg(L/K)$ as an A-module.*

For the proof of this we need a consequence from the classification of finitely generated modules for PIDs:

Theorem 1.19. *Let A be a PID and $M \neq 0$ a finitely generated torsionfree A-module. Then M is a free A-module of finite rank and every submodule $N \subseteq M$ is also free of rank $\leq \text{rk}_A M$.*

Proof of Theorem 1.18. Choose a basis $w_1, \dots, w_n \in B$ of L over K. Then by Thm (1.11) [wont be right] we have:

$$dB \subset Aw_1 + \dots + Aw_n \subset B$$

for some $0 \neq d \in A$. Then $Aw_1 + \dots Aw_n$ is free of rank n since the w_i are linearly independent over K and hence over A. Since A was a principle domain our previous theorem asserts that dB is a free A-module of rank $\leq n$. Since $B \cong dB$ as an A-module it is also free with the same estimate. But we also have $Aw_1 + \dots + Aw_n \subset B$ so $rk_A B \leq n$ and hence $\text{rk}_A B = n = \deg L/N$.Now Choose generators $e_1, \dots, e_r$ of $M \subset L$ as a B-module and choose some $0 \neq a \in A$ such that $ae_i \in B$ for all i. Then:

$$aM \subset B$$

so aM is a free A-module of rank $\leq \text{rk}_A B = n$ and hence so is M. The map:

$$B \to M \quad w \mapsto bw$$

is an injective map of A-modules. Hence we may view B as a submodule of M and thus $n = \text{rk}_A B \leq \text{rk}_A M$ and thus $\text{rk}_A M = n$. □

Corollary 1.20. *Let $K/\mathbb{Q}$ be a number field of degree n with ring of integers $\mathcal{O}_K$. Every finitely generated $\mathcal{O}_K$ submodule $\mathfrak{a} \neq 0$ of K is a free $\mathbb{Z}$-module of rank n. The discriminant $d(a_1, \dots, a_n)$ of a $\mathbb{Z}$ basis $\{a_i\}$ of $\mathfrak{a}$ depends only on $\mathfrak{a}$ and is denoted by $d(\mathfrak{a})$ We call*

$$d_k := d(\mathcal{O}_k)$$

the discriminant of K.

Proof. The first part is clear by the theorem since $\mathbb{Z}$ is a PID.
Let $b_1, \dots, b_n$ be another $\mathbb{Z}$-basis of $\mathfrak{a}$. Then there is an invertible matrix $(m_{ij}) = M \in \text{Gl}_n(\mathbb{Z})$ with. such that :

$$b_i = \sum_j m_{ij} a_j$$

hence:

$$\sigma(b_i) = \sum_j m_{ij} \sigma(a_j)$$

for all $\sigma \in \text{Hom}_{\mathbb{Q}}(K, \bar{Q}) = \{\sigma_1, \dots, \sigma_n\}$. Thus we have:

$$d(b_1, \dots, b_n) = \det((\sigma_k(b_i))_{k,i})^2 = (\det M \det(\sigma_k(b_i))_{k,i}) = (\det M)^2 d(a_1, \dots, a_n)$$

Since $M \in \text{Gl}_n(\mathbb{Z})$ we have that $\det M = \pm 1$ so we see that:

$$d(a_1, \dots, a_n) = d(b_1, \dots, b_n)$$

□

Example 1.21. $K/\mathbb{Q}$ quadratic, $K = \mathbb{Q}(\sqrt{d})$ for $1 \neq d \in \mathbb{Z}$ square-free. If d is not 1 in $\mathbb{Z}/4\mathbb{Z}$ the $\mathcal{O}_K \cong \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$, hence:

$$d_k = \begin{vmatrix} 1 & 1+\sqrt{d} \\ 1 & 1-\sqrt{d} \end{vmatrix} = 4d$$

For $d = 1 \in \mathbb{Z}/4\mathbb{Z}$, we have $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2}$ and thus we get:

$$d_k = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix} = d$$

2 Dedekind Rings

Definition 2.1 (/Theorem)**.** A ring R is called *Noetherian* if one of the following equivalent conditions hold:

1. Each nonempty set S of ideals in R has a maximal element
2. Every ascending chain of ideals in R is stationary.
3. Every ideal in R is finitely generated

Proof. 1) $\implies$ 2): Consider a a chain of ideals in R

$$I_1 \subset I_2 \subset \dots$$

By (1) the set $S = \{I_i | i \geq 1\}$ has a maximal element so the chain stabilizes.
(2) $\implies$ (3): Assume that I is not finitely generated. This immediately gives you an infinite ascending chain.
(3) $\implies$ (1): Assume that a nonempty set S of ideals in R has no maximal element. Then there exists a strictly ascending chain of ideals in the set S:

$$I_1 \subset I_2 \subset \dots$$

The union:

$$I = \bigcup_{i \geq 1} I_i$$

is an ideal in R and hence is finitely generated by (3). Thus it may be written as $I = (a_1, \dots, a_n)$ for some $a_1, \dots, a_n \in R$. Then there exists some $N \geq 1$ with $a_1, \dots, a_n \in I_N$ i.e. $I = I_N$ which is contradiction. □

Example 2.2.

1. Principle ideal domains are Noetherian, e.g. $R = \mathbb{Z}$
2. By Hilbert's Basis theorem:
   R Noetherian $\implies$ $R[X]$ Noetherian
3. $\mathbb{Q}[X_1, X_2, \dots]$ is not Noetherian.

Definition 2.3. A ring R is called a *Dedekind ring* iff:

1. R is an integrally closed domain
2. R is Noetherian.
3. Every prime ideal $\mathfrak{p} \neq 0$ is maximal

Example 2.4.

– Every principal domain is Dedekind, so in particular $\mathbb{Z}$
– Rings of integers are Dedekind [We will show this]

Theorem 2.5. *Let $K/\mathbb{Q}$ be a number field, then the ring of integers $\mathcal{O}_K$ is a Dedekind ring.*

Proof. Ad 2: Let $I \subset \mathcal{O}_K$ be an ideal. We've seen that as a $\mathbb{Z}$-module $\mathcal{O}_K$ is finitely generated and free. Hence the ideal $I \subset \mathcal{O}_K$ is also finitely generated as a $\mathbb{Z}$-module an thus also as an $\mathcal{O}_K$, i.e. $\mathcal{O}_K$ is Noetherian. Ad 1: Follows since $\mathbb{Z}$ is integrally closed and we've seen that integral closure is transitive Ad 3: Let $\mathfrak{p} \neq 0$ be a prime ideal. Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.
Claim: $\mathfrak{p} \cap \mathbb{Z} \neq 0$.
Indeed: Choose $0 \neq y \in \mathfrak{p}$. Then there exists an equation:

$$y^n + a_{n-1}y^{n-1} + \dots a_O$$

with $n \geq 1, a_i \in \mathbb{Z}$. We may assume that $a_o \neq 0$ (otherwise divide by a suitable power of y). Since $y \in \mathfrak{p}$ the equation implies that $a_0 \in \mathfrak{p} \cap \mathbb{Z} \neq 0$. Thus $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime p. Hence the map $\mathbb{Z} \hookrightarrow \mathcal{O}_K$ induces an inclusion:

$$\mathbb{Z}/p \hookrightarrow \mathcal{O}_K/\mathfrak{p}$$

and since $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, the ring $\mathcal{O}_K$ is a finitely generated $\mathbb{F}_p$-vector space. Consider $0 \neq \bar{x} \in \mathcal{O}\mathfrak{p}$. The $\mathbb{F}_p$-linear map:

$$\phi_{\bar{x}} : \mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}, \quad \bar{y} \mapsto \bar{x}\bar{y}$$

is injective since $\mathcal{O}_K/\mathfrak{p}$ is a domain. However it is also a finite dimensional $\mathbb{F}_p$-vector space this map is in fact an isomorphism. Consequently $\bar{x}$ is invertible and since it was arbitrary $\mathcal{O}_K/\mathfrak{p}$ is a field. □

Notations: R a domain, $K = \mathrm{Quot}(R)$, let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be R-submodules of K. We set:

- $\mathfrak{a}\mathfrak{b} :=$ R-submodule of K generated by all products ab with $a \in \mathfrak{a}, b \in \mathfrak{b}$
- $\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq R\}$

Facts:

- Associativity
- commutativity
- $\mathfrak{a}\mathfrak{a}^{-1} \subseteq T$
- $\mathfrak{a} \subseteq \mathfrak{b} \implies \mathfrak{b}^{-1} \subseteq \mathfrak{a}^{-1}$
- $\mathfrak{a}R \subset \mathfrak{a}$

For ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$ the product $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ is an ideal. We write $\mathfrak{a}|\mathfrak{b}$ if $\mathfrak{b} \subset \mathfrak{a}$. This is clearly transitive.
Fact: If $\mathfrak{p}$ is a prime ideal, then:

$$\mathfrak{p}|\mathfrak{a}\mathfrak{p} \implies \mathfrak{p}|\mathfrak{a} \text{ or } \mathfrak{p}|\mathfrak{b}$$

Proof. If $\mathfrak{p}$ divides neither then there exists some $a \in \mathfrak{a}$ with a not in $\mathfrak{p}$ and $n \in \mathfrak{b}$ with b not int $\mathfrak{p}$. Then since $\mathfrak{p}$is prime ab is not in $\mathfrak{p}$ and hence $\mathfrak{p}$ does no divide $\mathfrak{a}\mathfrak{b}$ □

Theorem 2.6. *Let R be a Dedekind ring. Then every ideal $0 \neq \mathfrak{a} \neq R$ can be written as a product of nonzero prime ideals:*

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i$$

This is unique up to ordering.

For the proof we need the following Lemma:

Lemma 2.7. *R a Dedekind ring with quotient field K. Then we have:*

1. *For every $\mathfrak{a} \neq 0$ in R there exists prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ with $\mathfrak{a}|\mathfrak{p}_1 \dots \mathfrak{p}_r$*
2. *if $\mathfrak{p} \neq 0$ is a prime ideal in R then for every ideal $\mathfrak{a} \neq 0$ we have :*

$$\mathfrak{a} \subsetneqq \mathfrak{a}\mathfrak{p}^{-1}$$

Proof. Proof of the Theorem using the Lemma Let $\mathcal{S}$ be the set of ideals $0 \neq \mathfrak{a} \neq R$ which do not have a decomposition into prime ideals as in the theorem. We claim that $\mathcal{S} = \varnothing$. Indeed, assume that $\mathcal{S} \neq \varnothing$, then since the ring is Noetherian $\mathcal{S}$ has a maximal element. Choose a maximal ideal $\mathfrak{p}$ containing $\mathfrak{a}$. Since $R \subset \mathfrak{p}^{-1}$ we get that:

$$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset R$$

Now by our Lemma we know that $\mathfrak{a} \subsetneqq \mathfrak{a}\mathfrak{p}^{-1}$ and $\mathfrak{p} \subsetneqq \mathfrak{p}\mathfrak{p}^{-1} \subset R$. Since $\mathfrak{p}$ was maximal in fact $\mathfrak{p}\mathfrak{p}^{-1} = R$ and since $\mathfrak{a}$ was maximal in clS we have that $\mathfrak{a}\mathfrak{p}^{-1}$ is not in $\mathcal{S}$. Note that $\mathfrak{a}\mathfrak{p}^{-1} \neq 0$ since $\mathfrak{a} \neq 0$ and $\mathfrak{a}\mathfrak{p}^{-1} \neq R$ [otherwise:

$$\mathfrak{a} = \mathfrak{a}R = \mathfrak{a}\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = R\mathfrak{p} = \mathfrak{p}$$

contradicting that $\mathfrak{a} \in \mathcal{S}$]. Thus there exist prime ideals $\mathfrak{p}_1, \dots \mathfrak{p}_r$ such that:

$$\mathfrak{a}\mathfrak{p}^{-1} = \prod_i \mathfrak{p}_i$$

hence:

$$\mathfrak{a} = \mathfrak{p} \prod_i \mathfrak{p}_i$$

Ad Uniqueness: Assume we have two decompositions

$$\mathfrak{a} = \prod_{i=0}^{r} \mathfrak{p}_i = \prod_{i=0}^{s} \mathfrak{q}_i$$

then $\mathfrak{p}_1 | \prod_i \mathfrak{q}_i$ and inductively we conclude that $\mathfrak{p}_1 | \mathfrak{q}_j$ for some j. By renumbering we may assume that $\mathfrak{p}_1 | \mathfrak{q}_1$ since $\mathfrak{q}_1$ is maximal. Then again by our lemma we have that:

$$\mathfrak{p}_1 \subsetneqq \mathfrak{p}_1\mathfrak{p}_1^{-1} \subset R$$

and by maximality the rightmost inclusion is an equality. Thus multiplying by $\mathfrak{p}_1^{-1}$ gives"

$$\prod_{i=1}^{r} \mathfrak{p}_i = \prod_{i=1}^{s} \mathfrak{q}_i$$

and inductively we see that $r = s$ and $\mathfrak{p}_i = \mathfrak{q}_i$ for all i. □

For the proof we needed the following Lemma:

Lemma 2.8. *If R is a Dedekind Ring, with Quotient field K, then the following hold:*

(a) For every ideal $0 \neq I$ in R there exists nonzero prime ideals $P_1, \dots, P_r$ such that:

$$I | P_1 \cdots P_r$$

(b) If P a nonzero prime ideal in R, then for every ideal $0 \neq I$ in R we have that:

$$I \subsetneqq IP^{-1}$$

Proof. (a) Let M be the set of ideals $I \neq 0$ which do not satisfy the assertion (a). We claim that $M = \emptyset$. Assume that $M \neq \emptyset$, since R Noetherian there exists a maximal $I \in M$. By definition of M, the ideal I cannot be prime. Hence there exist $b, c \in R$ with $bx \in I$ but b, c not in I. Set $J = I + (b)$ and $H = I + (c)$. Then $I \subsetneqq J$ and $I \subsetneqq H$ and $JH \subset I$, i.e. $I|JH$. We have that J, H are not in M since I was maximal in M. Thus we get can find primes P_i such that:

$$J \mid P_1 \cdots P_s \text{ and } H \mid P_{s+1} \cdots P_r$$

and hence:

$$I \mid P_1 \cdots P_r$$

Which is a contradiction. This shows that $M = \emptyset$

(b) We first show that $R \subsetneqq P^{-1}$ ("$\subset$" is clear). If $P = (a)$, then since $a \neq 0$ and $a^{-1} \in P^{-1}$. If $R = P^{-1}$, then $a^{-1} \in R$ and so a is a unit meaning $P = (a) = R$ which is a contradiction, so $R \subsetneqq P^{=1}$. Now assume that P is not principal. Choose some $0 \neq a \in P$. By part (a) there exits prime ideals $P_i \neq 0$ such that:

$$(a) \mid \prod_{i=1}^{r} P_i$$

Assume that r is minimal with this property. Then since P is prime we get that for some i:

$$P \mid (a) \implies P \mid P_i$$

and assume that $i = 1$. However since $P_1 \neq 0$ it is maximal (Since R was Dedekind) so we have that $P = P_1$. Moreover we have: $(a) \subsetneqq P$ i.e. (a) does not divide $P = P_1 \implies r \geq 2$. Since r was minimal (a) does not divide $P_2, \cdots, P_r$. Hence there exists some $b \in P_1 \cdots P_r$ which is not in (a) i.e. $a^{-1} \notin R$. On the other hand:

$$bP \subset PP_2 \cdots P_r = P_1 \cdots P_r$$

And thus :

$$a^{-1}bP \subset R \implies a^{-1}n \in P^{-1}$$

yielding $R \subsetneqq P^{-1}$.
Now for the general case: Let $I \neq 0$ be an ideal.
Claim: $I \subsetneq IP^{-1}$, only have to show that $I \neq IP^{-1}$ Assume: $I = IP^{-1}$
Since R is Noetherian have that $I = (a_1, \ldots, a_n)$ for $a_i \in R$. For each $x \in P^{-1}$ we get that:

$$xa_i = \sum_{j=1}^{n} r_{ij} a_j$$

Consider the AMtrix:

$$M = (x\delta_{ac} - r_{ij})_{i,j}$$

we see that :

$$M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0$$

For $d = \det M$ we get :

$$d \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = M^* M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0$$

Hence $d = 0$ since $I \neq 0$. Hence x is a zero of the monic polynomial:

$$f(t) := \det(T\text{id} - (r_i j)) \in R[T]$$

so $x \in K$ is integral over R and since R is integrally closed we have in fact $x \in R$. So we've seen that $P^{-1} \subset R$ so that $P^{-1} = R$ which is a contradiction to what we've shown in the first special case.

□

Remark 2.9. 1. By Theorem 2.3. (does not match) any ideal $0 \neq I \neq R$ in a Dedekind ring R can be written as :

$$I = \prod_{i=1}^{r} \mathfrak{P}_i^{\nu_i}$$

where the $\mathfrak{P}_i$ are the pairwise different prime ideals dividing I. This decomposition is unique up to ordering.

2. For ideals $I, J \notin \{0, R\}$ in any ring R we have:

$$I + J = R \iff \text{There is no prime ideal } P \text{ such that } P \mid a \text{ and } P \mid J$$

The ideals I in a ring R always form a commutative monoid under multiplication. If R is a Dedekind ring, using the more general construct of *fractional ideals* this monoid embeds into a group as follows:

Definition 2.10. Let R be a Dedekind ring, K its Quotient field. A fractional ideal of K is a finitely generated R-submodule $I \neq 0$ of K.

Remark 2.11. Let $0 \neq I \subset K$ be an R-submodule. Then I is a fractional ideal of K if and only if there exists some $0 \neq c \in R$ such that $cT \subset R$

Proof. If $I$is afractional ideal then it is generated by some elements $a_1, \ldots, a_n \in K$. choose some $0 \neq c \in R$ with $ca_i \in R$ for all i and so $cI \subset R$.
For the other direction assume that $cI \subset R$, since R is Noetherian the ideal cI is finitely generated. The isomorphism of R-modules $I \xrightarrow{\cdot c} cI$ shows that I is also finitely generated. □

Example 2.12. For $a \in K^{\times}$ we see that $(a) := aR$ is a fractional ideal.

In the discussion before the last Theorem we defined a multiplication on the set of R-submodules of K. The product of two fractional ideals is again a fractional ideal and we get a monoid. More is true:

Theorem 2.13. *Let R be a Dedekind ring with fraction field K. Then the monoid of fractional ideals of K is a group, called the ideal group $\mathfrak{I}_K$ of K. The unit is given by R and the inverse of $I \subset K$.*

$$I^{-1}\{x \in K \mid xI \subset R\}$$

Proof. I fractional implies that there exits some $0 \neq c \in R$ with $cI \subset R$, hence $c \in I^{-1} \neq 0$. Claim I^{-1} is finitely generated.
Have $I = (a_1, \ldots a_n)$ with wlog $a_1 \neq 0$. By definition we have $xa_1 \in R$ for all $x \in I^{-1}$ hence $a_1 I^{-1} \subset R$ which is an ideal an thus finitely generated i.e. $a_1 I^{-1} = (b_1,' \ldots b_m)$ for some $b_i \in R$. Hence $\frac{b_1}{a_1}, \ldots, \frac{b_m}{a_1}$ generates i^{-1} as an R-module. So we've shown that if I is a fractional ideal so is I^{-1} which actually holds in any Dedekind domain.
Claim: For a fractional ideal I we have that $II^{-1} = R$
We show this in three steps:

1. For $I = P$ a nonzero prime ideal. Then we've shown that $P \subsetneq PP^{-1} \subset R$ so $PP^{-1} = R$ since P was prime.

2. For any ideal $0 \neq I \subsetneq R$ we write I as a product of prime ideals:

$$I = \prod_{i=1}^{r} \mathfrak{P}_i$$

Set $J = \prod_{i=1}^{r} \mathfrak{P}_i^{-1}$. Then by (1) we have that $JI = R$. Also have that $J \subset I^{-1}$ by definition of the latter. For $x \in I^{-1}$ have that $xI \subset R$ so that $xJI \subset J$ but $xJ = xR$ and consequently $x \in J$, i.e. $I^{-1} \subset J$.

3. For a fractional ideal $I \in K$ there exits some $0 \neq x \in R$ with $xI \subset R$. For the ordinary ideal cI we have seen in (2) that $(cI)(cI)^{-1} = R$. It's easy to see that $(cI)^{-1} = c^{-1}I^{-1}$ and so II^{-1}.

□

We showed that fractional ideals have the form $\mathcal{L} = c^{-1}I$ for some $0 \neq c \in R$ and some ideal $I \subset R$.

Remark 2.14. Every fractional ideal $\mathcal{L}$ of K has a unique representation

$$\mathcal{L} = \prod \mathfrak{P}^{\nu_{\mathfrak{P}}} \quad \nu_{\nu_{\mathfrak{P}}} \in \mathbb{Z}$$

where $\nu_{\mathfrak{P}} = 0$ for almost all $\mathfrak{P}$ and the product runs over all prime ideals $\neq 0$ of R. Thus the group of fractional ideals $\mathcal{I}_K$ is a free abelian group on the set of non-zero primes of R.

Proof. There exists some $0 \neq c \in R$ with $c\mathcal{L} subset R$. Write

$$(c) = \prod \mathfrak{P}^{r_{\mathfrak{p}}} \quad r_{\mathfrak{P}} \in \mathbb{Z}_{\geq 0}$$

and:

$$c\mathcal{L} = \prod \mathfrak{P}^{s_{\mathfrak{P}}} \quad s_{\mathfrak{P}} \in \mathbb{Z}_{\geq 0}$$

Hence we get that:

$$\mathcal{L} = c^{-1}(c\mathcal{L}) = \prod \mathfrak{P}^{s_{\mathfrak{p}} - r_{\mathfrak{P}}}$$

and setting $\nu_{\mathfrak{P}} = s_{\mathfrak{P}} - r_{\mathfrak{P}} \in \mathbb{Z}$ gives existence. Uniqueness follows from multiplying any factorization with c. □

Definition 2.15. A fractional ideal is called principal if it is free of rank one i.e. $= aR$. These form a subgroup $\mathcal{P}_K$ of $\mathcal{I}_K$ The quotient:

$$\mathrm{Cl}_K := \mathcal{I}_K / \mathcal{P}_K$$

Is called the ideal class group of R

We have the basic exact sequence:

$$1 \to R^\times \to K^\times \to \mathcal{I}_K \to \mathrm{Cl}_K \to 1$$

So the "difference" between working with numbers $a \in K^\times$ and fractional ideals is controlled by the units $R^\times$ and the class group of Cl_K. If $R = \mathcal{O}_K$, $K/\mathbb{Q}$ a number field then it is known that:

1. $R^\times$ is a finitely generated abelian group (Dirichlet unit theorem)

2. Cl_K is finite

We will prove this in the next section using Minkowskis "geometry of numbers".
One more remark: In modern algebraic geometry the Class group is interpreted as $H^1(\mathrm{Spec}(R), \mathcal{O}^\times)$ the Picard group of the scheme $\mathrm{Spec}(R)$.

3 Minkowski Theory

Recall: A subset D of a topological space is called discrete if for every point $x \in D$ there is an open there is an open subset $x \in U \subset X$ such that $D \cap U = \{x\}$.

Example 3.1. – $\mathbb{Z} \subset \mathbb{R}$ is discrete and closed

– $D = \{\frac{1}{n} \mid n \geq 1\}$ is discrete in R [but not closed since $\bar{D} = D \cup \{0\}$]

Proposition 3.2. *Let X be a Hausdorff space and let $D \subset X$ be discrete and closed. Then for every compact subset $K \subset X$ the intersection $D \cap K$ is finite.*

Proof. Since D is discrete we have for all $x \in U_x \subset X$ with $D \cap U_x = \{x\}$. Since D is closed $X \setminus D$is open and hence:

$$(X \setminus D) \cup \bigcup_{x \in D} U_x = X$$

is an open covering thus since K is compact there exits $x_1, \dots, x_n \in D$ such that $K \subset (X \setminus D) \cup U_{x_1} \cup \dots U_{x_n}$ so we get that:

$$D \cap K \subset (D \cap U_{x_1}) \cup \dots \cup (D \cap U_{x_n}) = \{x_1, \dots, x_n\}$$

□

We will be interested in discrete subgroups Γ in finite dimensional $\mathbb{R}$-vector spaces V.

Remark 3.3. 1. $\mathbb{Z}^m \subset \mathbb{R}^n$ is a discrete subgroup.

2. $\mathbb{Z}[i] = \mathcal{O}_{\mathbb{Q}(i)} \subset \mathbb{C}$ is a discrete subgroup.

3. $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2} \subset \mathbb{R}$ is a subgroup but not discrete.
Fact: Any discrete subgroup $\Gamma \subset V$ is in fact closed.

Choose a norm $||-||$ on V and for $v \in V$ let:

$$U_\varepsilon(v) = \{w \in V \mid ||v - w|| < \varepsilon\}$$

which induces a topology on V as usual which does not depend on the choice of norm, since all norms on finite dimensional $\mathbb{R}$-vector spaces are equivalent.

Proof of Fact. Since $\Gamma \subset V$ is discrete there exists $\varepsilon > 0$ such that $\Gamma \cap U_\varepsilon(0) = \{0\}$. Assume $\gamma_n \to v$ is a convergent sequence with members $\gamma_n \in \Gamma$. Then (γ_n) is a Cauchy sequence, hence there is some $N = N_\varepsilon$ such that:

$$||\gamma_n - \gamma_m|| < \varepsilon \quad \text{for } m, n \geq N$$

i.e. $\gamma_n - \gamma_m \in \Gamma \cap U_\varepsilon(0) = \{0\}$. Thus $\gamma_n = \gamma_m$ for $m, n \geq N$ so $v = \gamma_N \in \Gamma$, so Γ is closed.(Here we've used that V is first countable so that we can check closedness via sequences). □

Questions: How to decide whether a given subgroup $Gamma \subset V$ is discrete? How do the discrete subgroups of V look?

Theorem 3.4. *A subgroup $\Gamma \subset V$ with $\dim_{\mathbb{R}} V < \infty$ is discrete iff there are $\mathbb{R}$-linearly independent vectors $v_1, \dots, v_m \in V$ which generate Gamma as a group. in This case we have that $\Gamma \cong \bigoplus_i \mathbb{Z}v_i$ is a free $\mathbb{Z}$-module of rank $m \leq n$.*

Remark 3.5. In our examples $\mathbb{Z}[\sqrt{2}]$ is a free $\mathbb{Z}$-module of rank $2 > 1 = n$. Hence it cannot be discrete by the theorem. Note that $1, \sqrt{2}$ are $\mathbb{Z}$-linearly independent but not $\mathbb{R}$-linearly.

Proof. If Γ is generated by $\mathbb{R}$-linearly independent $v_1, \ldots, v_m \in V$ choose $v_{m+1}, \ldots, v_n \in V$ such that the v_i form a basis of V. We show that $\Gamma \subset V$ is discrete. For

$$\gamma = \sum_{i=1}^{m} k_i v_i \in \Gamma$$

Set:

$$U\{\sum_{i=1}^{n} x_i v_i | x_i \in (k_i - \frac{1}{2}, k_i + \frac{1}{2} \text{ for } 1 \leq i \leq m \text{ and } x_i \in \mathbb{R}\}$$

Then $U \subset V$ is open, $\gamma \in U$ and in fact $\Gamma \cap U = \{\gamma\}$.
Let $\Gamma \subset V$ be discrete. Let $V' = \langle \Gamma \rangle$ be the $\mathbb{R}$-subspace generated by Γ and write $m = \dim V'$. Then there is an $\mathbb{R}$-basis $v_1, \ldots, v_m$ of V' such that $v_i \in Gamma$ for all i [Indeed, choose a basis $v'_1, \ldots v'_m$ of V', then each v'_i is an $\mathbb{R}$-linear combination of finitely many vectors in Γ. Thus a finite set of vectors in Γ generates V', so we take a maximal set of linearly independent vectors from this set to get a basis of V' consisting of vectors in Γ]. Set $\Gamma' = \bigoplus_i \mathbb{Z} v_i \subset \Gamma$, then we claim that:

$$\text{card}(\Gamma/\Gamma') < \infty$$

To see this write:

$$\Gamma = \coprod_{i \in I} \gamma_i + \Gamma'$$

where the $\gamma_i \in \Gamma$ for $i \in I$ are a system of representatives for Γ/Γ'. For the "fundamental domain":

$$\Phi := \{x_1 v_1 + \ldots x_m v_m \mid 0 \leq x_i < 1\}$$

we have that:

$$V' = \coprod_{\gamma' \in \Gamma'} \gamma' \Phi$$

Hence $\gamma_i = \gamma'_i + \mu_i$ with $\gamma' \in \Gamma'$ and $\mu_i \in Phi$, so $\mu_i \in \Gamma \cap \Phi$. Since Γ is discrete and closed in V and since $\bar{\Phi}$ is compact, the set $\Gamma \cap \bar{\Phi}$ is finite as we showed earlier. Hence the set of classes

$$gamma_i + \Gamma' = \mu_i + \Gamma', \quad i \in I$$

is finite i.e. I is finite. Thus $q := \text{card}(\Gamma/\Gamma')$ is finite as claimed. In particular we have that $q\Gamma \subset \Gamma'$. Therefore

$$\Gamma \subset \frac{1}{q}\Gamma' = \mathbb{Z}\frac{v_1}{q} \oplus \cdots \oplus \mathbb{Z}\frac{v_m}{q}$$

Hence Γ is a free $\mathbb{Z}$-module of rank $r \leq m$, i.e :

$$\Gamma = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_r$$

Since Γ generates the m-dimensional $\mathbb{R}$-vector space v' it follows that $r = m$ and moreover the w_i are an $\mathbb{R}$-basis of V', so in particular they are $\mathbb{R}$-linearly independent in V. □

Remark 3.6. Known: Every abelian group is the class group of some Dedekind Domain. Furthermore every finite abelian group is a quotient of the class group of a cyclotomic extension of $\mathbb{Q}$.

Definition 3.7. A discrete subgroup Γ of an n-dimensional $\mathbb{R}$-Vector space V is called a lattice if one of the following equivalent conditions holds:

1. $\text{rk}_{\mathbb{Z}}\Gamma = n$
2. There is an $\mathbb{R}$-basis of V which generates Γ as an abelian group.

3. There is a bounded (or compact) subset $M \subset V$ such that

$$V = \bigcup_{\gamma\in\Gamma} \gamma + M$$

Here the boundedness is defined with respect to some norm on V, which is well defined, since all norms on V are equivalent.
Indeed: We have already seen 1) $\iff$ 2).

Proof. (2) $\Longrightarrow$ (3) By assumption $\Gamma = \bigoplus_i \mathbb{Z}v_i$ for an $\mathbb{R}$-basis $\{v_i\}$ of V. The fundamental domain:

$$\Phi = \{v_1x_1 + \cdots + x_mv_m \mid 0 \le x_i < 1\}$$

is bounded and $\bar{\Phi}$ is compact. We have:

$$V \coprod_{\gamma\in\Gamma} \gamma + \Phi = \bigcup_{\gamma\in\Gamma} \gamma + \Phi$$

(3) $\Longrightarrow$ (1) Assume that $V = \bigcup_{\gamma\in\Gamma} \gamma + M$ for some bounded $M \subset M$. Let V' be the vector space generated by Γ
<u>Claim</u>: $V = V'$
Let $v \in V$ for every $k \ge 1$ we have $kv = \gamma_k + m_k$ with $\gamma_k \in \Gamma$ and $m_k \in M$. Hence we have:

$$V = \frac{1}{k}\gamma_k + \frac{1}{k}m_k$$

Since M is bounded $\lim_{k\to\infty} \frac{1}{k}m_k = 0$ and hence:

$$v = \lim_{k\to\infty} \frac{1}{k}\gamma_k$$

Since $\frac{\gamma_k}{k} \in V'$ which is closed in V, we have $v \in V'$. So we get $V \subseteq V'$ i.e. $V = V'$. It follows that $\mathrm{rk}_{\mathbb{Z}}\Gamma \ge n$. Using our theorem we know that $\mathrm{rk}_{\mathbb{Z}}\Gamma \le n$ since Γ was by assumption discrete so the rank is in fact $= n$ □

Remark 3.8. A discrete subgroup $\Gamma \subset V$ is a lattice iff the quotient V/Γ is compact.

Proof. We have that $\Gamma = v_1\mathbb{Z} \oplus v_m\mathbb{Z}$ where the v_i are $\mathbb{R}$-linearly independent with $m \le n = \dim V$. We can extend these to a basis $v_1, \dots v_n$ of V. then we have that:

$$\begin{aligned} V/\Gamma &\cong v_1\mathbb{R} \oplus \dots v_n\mathbb{R} \big/ v_1\mathbb{Z} \oplus \dots v_n\mathbb{Z} \\ &\cong \mathbb{R}/\mathbb{Z} \times \dots \mathbb{R}/\mathbb{Z} \times \mathbb{R} \times \cdots \times \mathbb{R} \\ &\cong (S^1)^m \times \mathbb{R}^{n-m} \end{aligned}$$

Hence this is compact iff $m = n$. □

<u>Notation</u>: Let Γ be a lattice in V with $\mathbb{Z}$-basis $v_1, \dots, v_n$. By our Theorem this is also an $\mathbb{R}$-basis of V. For the corresponding fundamental domain:

$$\Phi = \{\sum_{i=1}^n x_iv_i \mid 0 \le x_i < 1\}$$

We set:

$$\mathrm{vol}(\Gamma) := \lambda(\Phi)$$

where λ is the Lebesgue measure on V with respect to the $v_1, \dots, v_n$. In fact this is independent of the choice of v_i. Indeed, let $w_1, \dots, w_n$ be a another $\mathbb{Z}$-basis of Γ with corresponding fundamental domain Ψ. Let M be the matrix with $M(v_i) = w_i$ for all i. Then we have $M(\Phi) = \Psi$ and moreover M is unimodular i.e. $M \in \mathrm{GL}_n(\mathbb{R})$ and

$$M, M^{-1} \in \mathrm{M}_n(\mathbb{Z})$$

hence we have that:

$$\det M^{\pm 1} \in \mathbb{Z} \implies \det M \in \{\pm 1\}$$

and consequently:

$$\lambda(\Psi) = \lambda(M(\Phi)) = |\det M| \lambda(\Phi) = \lambda(\Phi)$$

Definition 3.9. A subset $X \subseteq V$ is called *centrally symmetric* if for all $x \in X$ we have $-x \in X$

Theorem 3.10 (Minkowski's lattice point theorem)**.** *Let Γ be a lattice in an n-dimensional euclidean vector space V and let $X \subseteq V$ be a centrally symmetric, convex Borel set. Assume that one of the following conditions holds:*

1. $\lambda(X) > 2^n \mathrm{vol}(\Gamma)$
2. *X is compact and* $\lambda(X) \geq 2^n \mathrm{vol}(\Gamma)$

Then X contains at least one point $0 \neq \gamma \in \Gamma$.

Example 3.11. $\Gamma = \mathbb{Z}^2 \subset \mathbb{R}^2, e_1 = (1,0), e_2 = (0,1), \Phi = (0,1)^2, \mathrm{vol}(\Gamma) = \lambda(\Phi) = 1$ Then the condition in the theorem means that $\lambda(X) > 2^2 = 4$. For our choice we have $\lambda(X) = 4$ but $X \cap \mathbb{Z}^2$, which shows that the strictness of the inequality is necessary in the non-compact case. In fact this counterexample works in every dimension.

Proof. It suffices to show that there exist $\gamma_1 \neq \gamma_2 \in \Gamma$ with:

$$D = (\gamma_1 + \frac{1}{2}X) \cap (\gamma_2 + \frac{1}{2}X)$$

Namely if $\xi \in D$ then:

$$\xi = \gamma_1 + \frac{12}{2}x_2 = \gamma_1 + \frac{1}{2}x_2$$

with $x_1, x_2 \in X$. The point:

$$0 \neq \gamma := \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1$$

lies on the line from $x_2 \in X$ to $-x_1 \in X$, hence since X is convex we have $\gamma \in X$. Assume that the sets $\gamma + \frac{1}{2}X$ for $\gamma \in Gamma$ are pairwise disjoint. Then we have:

$$\begin{aligned}
\Gamma = \lambda(\Phi) &\geq \lambda\left(\Phi \cap \coprod_{\gamma \in \Gamma} (\gamma + \frac{1}{2}X)\right) \\
&= \lambda\left(\coprod_{\gamma \in \Gamma} (\Phi \cap (\gamma + \frac{1}{2}X))\right) \\
&= \sum_{\gamma \in \Gamma} \lambda(\Phi \cap (\gamma + \frac{1}{2}X)) \\
&= \sum_{\gamma \in \Gamma} \lambda\left((\Phi - \gamma) \cap \frac{1}{2}X\right) \\
&\geq \lambda\left(\bigcup_{\gamma \in \Gamma} (\Phi - \gamma) \cap \frac{1}{2}X\right) \\
&= \lambda(\frac{1}{2}X) \quad \text{since} \coprod_{\gamma \in \Gamma} \Phi - \gamma = V \\
&= |\det(\cdot \frac{1}{2} : V \to V)| \lambda(X) = 2^{-n} \lambda(X)
\end{aligned}$$

This is a contradiction to the assumption $\lambda(X) > 2^{-n}\mathrm{vol}(\Gamma)$. This shows (i)
For (ii) and $\nu \geq 1$ set $X_\nu := (1+\frac{1}{\nu}X)$ Then X_ν is still a centrally symmetric, convex Borel set. Furthermore we have:

$$\lambda(X) = (1+\frac{1}{\nu}^n\lambda(X) > \lambda(X)) \geq 2^{-n}\mathrm{vol}(\Gamma)$$

By (i) we therefore get that $X_\nu \cap (\Gamma \setminus \{0\} \neq \varnothing)$. Now since X is compact and hence closed we see that:

$$\bigcap_{\nu\geq 1} X_\nu = X$$

now the sets $X_\nu \cap (\Gamma \setminus \{0\})$ are closed in V and hence in X_1. Since X was compact so is X_1 and we get that the following intersection of non-empty closed sets:

$$\bigcap_{\nu\geq 1} X_\nu(\Gamma\setminus\{0\}) = X \cap (\Gamma \setminus \{0\})$$

is again non-empty. □

Let $K/\mathbb{Q}$ be a number field of degree n. We know that there are m pairwise different embeddings:

$$\sigma : K \hookrightarrow \mathbb{C}$$

Let $c : \mathbb{C} \to \mathbb{C}$ be the complex conjugation, then if σ is an embedding $\bar{\sigma} := c \circ \sigma$ is an embedding. We call σ a *real* embedding if $\bar{\sigma} = \sigma$. Denote by r_1 the number of real embedings of K. The non-real embedings appear in pairs $\sigma, \bar{\sigma}$ hence there is some $r_2 \in \mathbb{Z}_{\geq 0}$ such that $2r_2$ is the number of non-real embeddings of K. We have that $n = r_1 + 2r_2$ is the total number of embedings. Usual one says "complex" for "non-real". Let $\sigma_1, \dots, \sigma_{r_1}$ be the real embeddings and $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+1}, \dots, \bar{\sigma}_{r_1+r_2}$ the complex embeddings. Set

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \dots, \sigma_{r_1+r_2}(x))$$

The map:

$$\sigma : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \mathbb{R}^n$$

is called the "canonical embedding of K".
More invariantly this is the map:

$$K \to K \otimes_{\mathbb{Q}} \mathbb{R}$$

Proposition 3.12. *Let $M \subset K$ be a free $\mathbb{Z}$-module of rank n. Then $\sigma(M)$ is a lattice in $\mathbb{R}^n$ and we have:*

$$\mathrm{vol}\sigma(M) = 2^{-r_2}|d(M)|^{\frac{1}{2}}$$

where $d(M) = (\det((\sigma_i(x_j))_{i,j})^2$ for any $\mathbb{Z}$ basis $x_1, \dots, x_n$ of M is the discriminant of M.

Proof. Identifying $R^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ we have:

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_!}, \mathrm{Re}\sigma_{r_1+1}(x), \mathrm{Im}\sigma_{r_1+1}(x), \dots, \mathrm{Im}\sigma_{r_1+r_2}(x)$$

Let D be the determinant with rows $\sigma(x_1), \dots, \sigma(x_n)$ then we have that:

$$D = \pm(2i)^{-r_2}\det((\sigma_i(x_j))_{i,j})$$

[Here's the argument in the case $r_1 = 0, r_2 = 1$ which shows how to proceed in general. In this case $\sigma(x) = (\mathrm{Re}\sigma_1(x), \mathrm{Im}\sigma_1(x)$ and:

$$D = \begin{vmatrix}\sigma(x_1)\\ \sigma(x_2)\end{vmatrix} = \begin{vmatrix}a_1 & b_1\\ a_2 & b_2\end{vmatrix} = \frac{1}{i}\begin{vmatrix}a_1 & ib_1\\ a_2 & ib_2\end{vmatrix} = \frac{1}{2i}\begin{vmatrix}a_1+ib_1 & 2ib_1\\ a_2+ib_2 & 2ib_2\end{vmatrix} = \frac{-1}{2i}\begin{vmatrix}\sigma_1(x_1) & \bar{\sigma}_1(x_1)\\ \sigma_1(x_2) & \bar{\sigma}_2(x_2)\end{vmatrix}$$

Thus since $d(M) \neq 0$ we get $D \neq 0$ so the vectors $\sigma(x_1), \ldots, \sigma(x_n)$in $\mathbb{R}^n$ are $\mathbb{R}$-linearly independent and hence $\sigma(M)$ is a lattice. Let T be the matrix with rows $\sigma(x)i$. If:

$$E = \{\sum_i t_i e_i \mid 0 \leq t_i < 1\} \subset \mathbb{R}^n$$

then $T(E)$ is a fundamental domain Φ for the lattice $\sigma(M)$ hence:

$$\begin{aligned} \mathrm{vol}(\sigma(M)) &= \lambda(T(E)) = \det(T)\mathrm{vol}(E) \\ &= \det(T)D = 2^{-r2}\det(\sigma_i(x_j)) = 2^{-r_2}d(M)^{\frac{1}{2}} \end{aligned}$$

□

Before we can proceed we need the so called *norm* of an ideal.

Setup:

$K/\mathbb{Q}$ number field, $\deg(K/\mathbb{Q}) = n$, $R = \mathcal{O}_K$, $N(x) := |N_{K/\mathbb{Q}}(x)|$ for $x \in K$

Proposition 3.13. *For $x \in R$, $x \neq 0$ we have that $N(x) = |R/x|$.*

Proof. We have that $xR \cong R$ are both free $\mathbb{Z}$-modules of rank n. By the elementary divisor theorem applied to the inclusion:

$$Rx \subseteq R$$

there exists a $\mathbb{Z}$-basis $e_1, \ldots, e_n$ of the $\mathbb{Z}$-module R and elements $d_1, \ldots, d_n \in \mathbb{Z}$ with $d_i \geq 1$ such that $d_1e_1, dots, d_ne_n$ is a basis of Rx. As abelian groups we therefore have an isomorphism:

$$R/x \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$$

so we see that:

$$|R/x| = d_1 \cdots d_n$$

Let $\phi_x : K \to K$ be the multiplication by x. Then by definition we had that:

$$N(x) = |\det(\phi_x)|$$

We write $\phi_x = \psi \circ \phi$ where:

$$\begin{aligned} \phi :&K \xrightarrow{\sim} K \\ &e_i \mapsto d_ie_i \end{aligned} \qquad\qquad \begin{aligned} \psi : &K \xrightarrow{\sim} K \\ &d_ie_i \mapsto xe_i \end{aligned}$$

Then $\det(\psi) = d_1 \cdots d_n$ and $\phi(R) = Rx$ and moreover $\psi(Rx) = Rx$ hence $\det(\psi) = \pm 1$ since ψ is unimodular. Thus we find that:

$$N(x)|\det(\phi_x)| = |\det(\psi)||\det(\phi)| = d_1 \cdots d_n = |R/x|$$

□

Definition 3.14. For an ideal $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ the number:

$$N(\mathfrak{a} := |\mathcal{O}_K/\mathfrak{a}|$$

is called the *norm* of $\mathfrak{a}$

Remark 3.15. 1. For $0 \neq a \in \mathfrak{a}$ have $\mathcal{O}_K a \subset \mathfrak{a}$ hence there is a surjection:

$$\mathcal{O}/a \to \mathcal{O}_K/\mathfrak{a}$$

and thus :

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|| \leq \mathcal{O}_K/a| = N(a)$$

is finite.

2. For a principal ideal $\mathfrak{a} = (a)$ we have seen that:

$$N(\mathfrak{a}) = N(a)$$

Proposition 3.16. *For two non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ we have that:*

$$N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b})$$

Proof. Since $\mathfrak{b} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ for some nonzero prime ideals $\mathfrak{P}_i$, it suffices to show that:

$$N(\mathfrak{a}\mathfrak{P}) = N(\mathfrak{a})N(\mathfrak{P})$$

for all nonzero prime ideal $\mathfrak{P} \subset \mathcal{O}_K$. Note that these are in particular maximal. Since $\mathfrak{a}\mathfrak{P} \subset \mathfrak{a}$ we have that:

$$R/\mathfrak{a} \cong {}^{R/\mathfrak{a}\mathfrak{P}}\!\big/_{\mathfrak{a}/\mathfrak{a}\mathfrak{P}}$$

as abelian groups, hence we see that:

$$|R/\mathfrak{a}\mathfrak{P}| = |R/\mathfrak{a}| \cdot |\mathfrak{a}/\mathfrak{a}/\mathfrak{P}|$$

i.e.:

$$N(\mathfrak{a}\mathfrak{P}) = N(\mathfrak{a})|\mathfrak{a}/\mathfrak{a}\mathfrak{P}|$$

<u>Claim</u>: $|\mathfrak{a}/\mathfrak{a}\mathfrak{P}| = |R/\mathfrak{P}|$ We may view $\mathfrak{a}/\mathfrak{a}\mathfrak{P}$ as a vector space over the (in fact finite) field $R/\mathfrak{P}$. We have a bijection between ideals $\mathfrak{Q} \subset R$ with $\mathfrak{a}\mathfrak{P} \subset \mathfrak{Q} \subset \mathfrak{a}$ with the $R/\mathfrak{P}$ sub vector spaces of A/AP. The unique decomposition into prime ideals implies that either $\mathfrak{Q} = \mathfrak{a}$ or $\mathfrak{Q} = \mathfrak{a}\mathfrak{P}$ hence $\mathfrak{a}/\mathfrak{a}\mathfrak{P}$ has no non-trivial subspaces thus it is one dimensional i.e. $\mathfrak{a}/\mathfrak{a}\mathfrak{P} \cong R/\mathfrak{P}$ which proves the claim. □

Back to Minkowski Theory:

Corollary 3.17. *Let K be a number field with discriminant $d = d_{K/\mathbb{Q}}$ and let $\mathfrak{a} \neq 0$ be and ideal in $\mathcal{O}_K$. then $\sigma(\mathcal{O}_K)$ and $\sigma(\mathfrak{a})$ are lattices in $\mathbb{R}^n$ under the canonical embedding $\sigma : K \to \mathbb{R}^n$ and moreover we have:*

$$\mathrm{vol}(\sigma(\mathcal{O}_K)) = 2^{-r_2}|d|^{1/2}$$
$$\mathrm{vol}(\sigma(\mathfrak{a})) = 2^{-r_2}|d|^{1/2}N(\mathfrak{a})$$

Proof. Since both $\mathcal{O}_K$ and $\mathfrak{a}$ are free $\mathbb{Z}$-modules of rank $n = \deg(K/\mathbb{Q})$ in K we have already seen that $\sigma(\mathcal{O}_K)$ and $\sigma(\mathfrak{a})$ are lattices and that the formula for $\mathrm{vol}(\sigma(\mathcal{O}_K))$. Furthermore we have that:

$$\mathcal{O}_K/\sigma \xrightarrow{\sim} \sigma(\mathcal{O}_K/\sigma(\mathfrak{a})$$

hence the index of the lattice $\sigma(\mathfrak{a})$ in the lattice $\sigma(\mathcal{O}_K)$ is $N(\mathfrak{a})$. It follows that:

$$\mathrm{vol}(\sigma(\mathfrak{a}) = N(\mathfrak{a})\mathrm{vol}(\sigma(\mathcal{O}_K))$$

This follows form the following general argument: Let $\Gamma' \subset \Gamma \subset V$ be lattices in a euclidean vector space V. Choose a $\mathbb{Z}$-basis $v_1, \ldots, v_n \in \Gamma$ such that $d_1v_1, \ldots, d_nv_n$ is a $\mathbb{Z}$-basis opf Γ' for suitable $d_i \in \mathbb{Z}$ with $d_i \geq 1$. Then:

$$\Gamma/\Gamma' \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$$

hence $|\Gamma/\Gamma'| = d_1 \cdots d_n$ if Ψ is a fundamental domain of Γ. Then $\phi(\Phi)$ is a fundamental domain for Γ' where ϕ is the linear map defined via $\phi(v_i) := d_iv_i$. Thus we get:

$$\mathrm{vol}(\Gamma') = \lambda(\phi(\Phi)) = |\det(\phi)|\lambda(\Phi) = d_1 \cdots d_n\lambda(\Phi) = |\Gamma/\Gamma'|\mathrm{vol}(\Gamma)$$

□

Theorem 3.18. *Let $K/\mathbb{Q}$ be a number field of degree $n = r_1 + 2r_2$ and discriminant $d = d_{K/\mathbb{Q}}$. For every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}_K$ there exists some $0 \neq x \in \mathfrak{a}$ with:*

$$|N_{K/\mathbb{Q}}(x)| \leq (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} |d|^{1/2} N(\mathfrak{a})$$

Proof. Let $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be the canonical embedding. For $t > 0$ let

$$X_t := \left\{ (y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2} \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t \right\}$$

Then X_t is compact, convex and centrally symmetric with:

$$\lambda(X_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t}{n!}$$

Choose t such that:

$$\lambda(X_t) = 2^n \mathrm{vol}(\sigma(\mathfrak{a}))$$

i.e.:

$$2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{2!} = 2^{n-r_2} |d|^{1/2} N(\mathfrak{a})$$

equivalently:

$$t^n = 2^{n-r_1} \pi^{-r_2} n! |d|^{1/2} N(\mathfrak{a})$$

so this is solvable. Now by Minkowskis theorem there exits some $0 \neq w \in \sigma(\mathfrak{a}) \cap X_t$. Let $0 \neq x \in \mathfrak{a}$ be the element with $\sigma(x) = w$. Using the inequality of the geometric and the arithmetic mean:

$$\sqrt[n]{a_1 \cdots a_n} \leq \frac{1}{n}(a_1 + \cdots + a_n) \text{ for } a_i \geq 0$$

we find by setting $w_{i+r_2} = \bar{w}_i$ for $r_1 + 1 \leq i \leq r_2$ that:

$$\begin{aligned} |N_{K/\mathbb{Q}}(x)| &= \prod_{i=1}^{n} |\sigma_i(x)| = \prod_{i=1}^{n} |w_i| \\ &\leq \left(\frac{1}{n} \sum_{i=1}^{n} |w_i| \right)^n \\ &= \frac{1}{n^n} \left(\sum_{i=1}^{r_1} |w_i| + 2 \sum_{i=r_1+1}^{r_1+r_2} |w_i| \right)^n \leq \frac{t^n}{n^n} \end{aligned}$$

Now plugging in our choice of t and the fact that $n = r_1 + 2r_2$ we get the claim. □

Corollary 3.19. *Let K be a number field of degree $n = r_1 + nr_2$ and discriminant $d = d_{K/\mathbb{Q}}$. Then every ideal class in $\mathrm{Cl}_K = \mathcal{I}_K / \mathcal{P}_K$ contains an ideal $\mathfrak{b} \subset \mathcal{O}_K$ such that:*

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}$$

Proof. Let $\mathfrak{k} \in \mathrm{Cl}_K$ and $\mathfrak{a}' \in \mathfrak{k}$. We may assume that $\mathfrak{a} = (\mathfrak{a}')^{-1} \subseteq \mathcal{O}_K$. By the previous theorem there exists some $0 \neq x \in \mathfrak{a}$ such that:

$$|N(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |s|^{1/2} N(\mathfrak{a})$$

By definition of $\mathfrak{a}^{-1}$ we see that $\mathfrak{b} := x\mathfrak{a}^{-1} \subset \mathcal{O}_K$. Moreover $\mathfrak{b} = (x)\mathfrak{a}' \in \mathfrak{k}$ and:

$$N(\mathfrak{b}) = N(x) N(\mathfrak{a}') = |N(x)| N(\mathfrak{a})^{-1} \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}$$

□

Corollary 3.20. *Let $K/\mathbb{Q}$ be a number field of degree n with discriminant d, then for $n \geq 2$ we have:*

$$|d| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1} \equiv n \leq \frac{\log(|d|)+\log(\frac{9}{4})}{\log(\frac{3\pi}{4})}$$

and hence:

$$n \leq C\log(|d|)$$

for some constant independent of K.

Proof. In the previous corollary we have $N(\mathfrak{b}) \geq 1$ and hence:

$$|d| \geq \left(\frac{\pi}{4}\right)^{2r_2}\frac{n^{2n}}{(n!)^2} \geq \left(\frac{\pi}{4}\right)^{n}\frac{n^{2n}}{(n!)^2} =: a_n$$

and hence using the binomial formula we get:

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} \geq \frac{\pi}{4}\left(1+2n\frac{1}{n}+\geq 0\right) \geq \frac{3\pi}{4}$$

and thud:

$$|d| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2} = \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

□

As an obvious consequence we get:

Theorem 3.21 (Hermite-Minkowski)**.** *For every number field $K \neq \mathbb{Q}$ we have that $|d_{K/\mathbb{Q}}| \geq 2$*

Theorem 3.22. *For every number field $K/\mathbb{Q}$ the class number $L_K = |\mathrm{Cl}_K|$ is finite*

Proof. It suffices to show that for every integer $N \geq 1$ there are only finitely many ideals $\mathfrak{b} \subset \mathcal{O}_K$ with $N(\mathfrak{b}) = N$. Since $|\mathcal{O}_K/\mathfrak{b} = N(\mathfrak{b}) = N|$ we have that $N = 0 \in \mathcal{O}_K/\mathfrak{b}$ i.e. $N\mathcal{O}_K \subset \mathfrak{b}$. Now let $\mathfrak{P}_1 \cdots \mathfrak{P}_r$ be the the prime decomposition of $N\mathcal{O}_K$ into prime ideals. Then the possible ideals $\mathfrak{b}$ are precisely the partial products of the ideals $\mathfrak{P}_i$ and thus there are only finitely many. □

Theorem 3.23 (Hermite)**.** *There are only finitely many number fields for a given discriminant.*

Proof. Fix some $d \in \mathbb{Z}$, then if $d_{K/\mathbb{Q}} = d$ there are only finitely many possibilities of $n = \deg K/\mathbb{Q}$ and hence for r_1, r_2. Therefore it suffices to prove the following assertion:
Given d, n, r_1, r_2 there are only finitely many number fields K with:

$$d_{K/\mathbb{Q}} = d,\ \deg(K/\mathbb{Q}) = n,\ r_1(K) = r)_1,\ r_2(K) = r_2$$

To see this consider the following subset $B \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$:

1.Case If $r_1 \geq 1$ set:

$$B = \left\{(x,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |y_1| \leq 2^n \left(\frac{2}{\pi}\right)^{r_2} |d|^{1/2},\ |y_i| \leq \frac{1}{2}\ i > 1,\ |z_j| \leq \frac{1}{2}\ j \geq 1\right\}$$

2.Case If $r_1 = 0$ set:

$$B = \left\{z \in \mathbb{C}^{r_2} \mid |\mathrm{Im}(z_!)| \leq 2^n \left(\frac{2}{\pi}\right)^{r_2-1} |d|^{1/2},\ |\mathrm{Re}(z_1)| \leq \frac{1}{4},\ |z_j| \leq \frac{1}{2}\ 2 \leq j \leq r_2\right\}$$

then B is closed, convex and centrally symmetric of Lebesgue measure:

$$\lambda(B) = 2^{n+1-r_2}|d|^{1/2}$$

Now let $\sigma : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be the canonical embedding. We have that:

$$\mathrm{vol}(\sigma(\mathcal{O}_K)) = 2^{-r_2}|d|^{1/2}$$

and hence:

$$\lambda(B) = 2^{n+1}\mathrm{vol}(\sigma(\mathcal{O}_K)) > 2^n\mathrm{vol}(\sigma(\mathcal{O}_K))$$

Then there exists some $0 \neq x \in \mathcal{O}_K$ with $\sigma(x) \in B$.
Claim 1: $K = \mathbb{Q}(x)$
(This is equivalent to asking that $\sigma_i(x) \neq \sigma_j(x)$ for $i \neq j$)

1.Case If $r_1 \geq 1$ consider the inequality:

$$1 \leq |N(x)| = \prod_{i=1}^{n} |\sigma(x)|$$

by definition of B we have that $\sigma_i(x) \leq 1/2$ for $i \geq 2$ and hence we get:

$$|\sigma_1(x)| \geq 2^{n-1} \geq 1$$

Thus $\sigma_1(x) \neq \sigma_i(x)$ for all $i \geq 2$. Now take a Galois extension $K \subset L \subset \mathbb{C}$, then applying the automorphisms of L to the inequalities we find that:

$$\sigma_\nu(x) \neq \sigma_\mu(x)$$

for all $\nu \neq \mu$ and hence x is primitive.

2.Case If $r_1 = 0$ we may assume that in our ordering $\sigma_1, \dots, \sigma_n$ we have that $\sigma_2 = \bar{\sigma}_1$. By definition of B we then have $\sigma_i(x) \leq 1/2$ for $3 \leq i \leq n$ and so we get that:

$$|\sigma_1(x)^2| = |\sigma_1(x)||\sigma_2(x)| \geq 2^{n-2} \geq 1$$

and hence $|\sigma_1(x)| = |\sigma_2(x)| \geq 1$ and therefore $\sigma_1(x) \neq \sigma_i(x)$ for $3 \leq i \leq n$. Thus it remains to show that $\sigma_1(x) \neq \sigma_2(x) = \bar{\sigma}_1(x)$. By definition of B we have that $\mathrm{Re}(\sigma_1(x)) \leq 1/4$. Since $|\sigma_1(x)| \geq 1$ we see that $\sigma_1(x) \neq \mathrm{Re}(\sigma_1(x))$ i.e. that $\sigma_1(x) \notin \mathbb{R}$ ans so $\sigma_1(x) \neq \bar{\sigma}_1(x)$ as claimed.

Using Claim 1 the theorem will follow from:
Claim 2: Given d, n, r_1, r_2 the set of algebraic integers $x \in \mathbb{C}$ which arise from the construction above is finite.
Indeed: By construction of our set B there is a constant $C(d, n, r_2)$ such that $|\sigma_i(x)| \leq C$ for all $1 \leq i \leq n$. Consider the minimal polynomial of x:

$$m_x(T) = \prod_{i=1}^{n}(T - \sigma_i(x)) = \sum_{\nu=0}^{n} c_\nu T^\nu$$

with $c_\nu \in \mathbb{Z}$ since $x \in \mathcal{O}_K$. Furthermore these c_ν are the elementary symmetric functions of $\sigma_1(x), \dots, \sigma_n(x)$. Hence there is another constant $D = D(d, n, r_2)$ such that $|c_\nu| \leq D$ for all $0 \leq \nu \leq n$. Hence there are at most $(2D+1)^{n+1}$ possibilities for $m_x(T)$ and hence for x. □

Next we study the structure of the group of units $\mathcal{O}_K^\times$ for a number field K. The basic result is this:

Theorem 3.24 (Dirichlet's unit theorem)**.** *For a number field K set $r = r_1 + r_2 - 1$ Then we have:*

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^r$$

Where μ_K is the finite cyclic group of roots of unity in K. Thus there are r units $\eta_1, \ldots, \eta_r \in \mathcal{O}_K$ such that every unit $u \in \mathcal{O}_K^\times$ has a unique representation of the form:

$$u = \zeta \eta_1^{n_1} \ldots \eta_r^{n_r}, \quad n_i \in \mathbb{Z},\ \zeta \in \mu_K$$

Remark 3.25. Except in special cases there are no known explicit formulas for the generators of the free part (called *fundamental units*)

Example 3.26. 1. K imaginary quadratic $r = 0 + 1 - 1 = 0$, hence $\mathcal{O}_K^\times = \mu_K$

2. K real quadratic, $r = 2 + 0 - 1 = 1$ hence:

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z} = \{\pm 1\} \times \mathbb{Z}$$

3. $K = \mathbb{Q}(\zeta_p)$ for $p \geq 3$ and ζ_p a primitive p-th root of unity. Then $r_1 = 0$, $r_2 = \frac{p-1}{2}$ i.e. $r = \frac{p-3}{2}$ and therefore:

$$\mathcal{O}_K^\times \cong \mu_{2p} \times \mathbb{Z}^{\frac{p-3}{2}}$$

Proof. We first show that $\mathcal{O}_K^\times$ is a finitely generated abelian group and then we determine the rank. For this consider the so called *logarithmic embedding*:

$$L : K^\times \to \mathbb{R}^{r_1+r_2}$$
$$L(x) = (\log(|\sigma_1(x)|), \ldots, \log(|\sigma_{r_1+r_2}(x)|)$$

which one obtains from the canonical embedding σ.

Claim 1 Let $B \subset \mathbb{R}^{r_1+r_2}$ be bounded, then the set:

$$B' := L^{-1}(B)$$

is finite

Proof. Since B is bounded there exist $\varepsilon > 0$, $C > 0$ such that for all $x \in Bp$ we have:

$$\varepsilon \leq |\sigma_i(x)| \leq C$$

for $i = 1, \ldots, r_1 + r_2$ and hence for all $i = 1, \ldots, n$. Now let:

$$m_x(T) = \sum_{\nu=0}^{d_x} c_\nu T^\nu$$

be the minimal polynomial of x. Then we have that:

(a) $d_x \leq n = \deg(K/\mathbb{Q})$

(b) $m_x(T) \in \mathbb{Z}[T]$ since $x \in \mathcal{O}_K$

(c) There is a constant $D = D_{K,B}$ such that

$$|c_\nu| \leq D \text{ for } 0 \leq \nu \leq d_x$$

since the c_ν are the elementary symmetric functions of a subset of $\sigma_1(x), \ldots, \sigma_n(x, y)$. Hence there are only finitely many possibilities for $m_x(T)$ so also for x.

□

Consequences:

(a) The subgroup $\Gamma = L(\mathcal{O}_K^\times \subset \mathbb{R}^{r_1+r_2}$ is discrete
(b) $\ker L = \mu_K$ is a finite cyclic subgroup of $\mathcal{O}_K^\times$

Proof. ad (a): Fix a norm on $\mathbb{R}^{r_1+r_2}$. for $v \in \Gamma$ the $\varepsilon = 1$ ball $U_1(v)$ contains only finitely many elements of Γ by Claim 1. For small enough $0 < \varepsilon \leq 1$ we therefore have:

$$U_\varepsilon(v) \cap \Gamma = \{v\}$$

thus Γ is discrete.
ad (b): For $B = \{0\}$ Claim 1 asserts that the following subgroup of $\mathcal{O}_K^\times$ is finite:

$$\{x \in \mathcal{O}_K^\times \mid L(x) = 0\}$$
$$\{x \in \mathcal{O}_K^\times \mid |\sigma_i(x)| = 1 \text{ for all } 1 \leq i \leq n\}$$

Hence:

$$\ker(L|_{\mathcal{O}_K^\times} \subset \mu_K)$$

since all elements have finite order. ON the other hand for $\zeta \in \mu_K$ we have in fact $\zeta \in \mathcal{O}_K^\times$ since ζ, ζ^{-1} are roots of the monic polynomial $T^n - 1$. Moreover $\sigma_i(\zeta)$ is again a root of unity in $\mathbb{C}$ and thus $|\sigma_i(\zeta)| = 1$ for all i i.e. we see that $\zeta \in \ker(L|_{\mathcal{O}_K^\times})$. So in conclusion

$$\ker(L|_{\mathcal{O}_K^\times}) = \mu_K$$

and this group is finite. Furthermore all finite subgroups of $K^\times$ are cyclic. □

Now the discrete subgroup $\Gamma = L(\mathcal{O}_K^\times) \subset \mathbb{R}^{r_1+r_2}$ is free of rank $\leq r_1 + r_2$. Since $\mu_K \subset \mathcal{O}_K^\times$ is finite and L induces an isomorphism:

$$\mathcal{O}^\times / \mu_K \xrightarrow{\sim} \Gamma$$

the abelian group $\mathcal{O}_k^\times$ is finitely generated of rank $\leq r_1 + r_2$ with torsion part μ_K. In fact more is true:

1. Claim 2: We have $\mathrm{rk}\mathcal{O}_K^\times \leq r_1 + r_2 - 1 = r$

Proof. For $x \in \mathcal{O}_K^\times$ we know that:

$$N_{K/\mathbb{Q}}(x) \in \mathbb{Z}^\times\{\pm 1\}$$

□

$$1 = \prod_{i=1}^{n} |\sigma_i(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(x)|^2$$

and therefore:

$$0 = \sum_{i=1}^{r_1} \log(|\sigma_i(x)|) + 2 \sum_{i=r_1+1}^{r_2+r_1} \log(\sigma_i(x))$$

Thus the discrete subgroup $\Gamma = L(\mathcal{O}_K^\times)$ lies in the hyperplane:

$$W = \left\{ y \in \mathbb{R}^{r_1+r_2} \mid \sum_{i=1}^{r_1} y_i + 2 \sum_{i=r_1+1}^{r_1+r_2} y_i = 0 \right\}$$

Since Γ is discrete in $\mathbb{R}^{r_1+r_2}$ it also discrete in W and we get that:

$$\mathrm{rk}\Gamma \leq \mathrm{dim} W = r = r_1 + r_2 - 1$$

Claim 3 In fact $\mathrm{rk}\mathcal{O}_K^\times = \mathrm{rk}\Gamma = r$ i.e. Γ is a lattice in W. This will follow from:

Claim 3* For any $0 \neq \phi \in W^\vee$ there exists some $u \in \mathcal{O}_K^\times$ with $\phi(L(u)) \neq 0$ Indeed: Suppose we have shown this and denote by $\langle\Gamma\rangle = W$ the $\mathbb{R}$-subvectorspace generated by Γ. Since Γ is a discrete subgroup in W we know that:

$$\mathrm{rk} = \dim_{\mathbb{R}}\langle\Gamma\rangle$$

Now if $\mathrm{rk}\Gamma < r$ (i.e. Clam 3 is wrong), then $W/\langle W\rangle \neq 0$ and hence there is a surjective linear map:

$$\psi : W/\langle\Gamma\rangle \to \mathbb{R}$$

The composition:

$$\phi : W \to W/\langle\Gamma\rangle \xrightarrow{\psi} \mathbb{R}$$

is again surjective hence defines nonzero element in $W^\vee$ such theta $\phi(\Gamma) = 0$. Hence by Claim 3* there exists $\gamma = L(u) \in \Gamma$ such hat $\phi(\gamma) \neq 0$ which is a contradiction. Thus Claim 3 holds in this case.

Proof of Claim 3*. For any $0 \neq \phi \in W^\vee$ there are $c_1, \dots c_r \in \mathbb{R}$ where $r = r_1 + r_2 - 1$ and $(c_1, \dots c_r) \neq 0$ such that:

$$\phi(y) = c_1 y_1 + \cdots + c_r y_r \qquad \text{for all } y \in W$$

Since we had:

$$\sum_{i=1}^{r_1} y_i + 2\sum_{i=r_1+1}^{r_1+r_2} y_i = 0$$

Now fix $\alpha \in \mathbb{R}$ with $\alpha > 2^n \mathrm{vol}(\sigma(\mathcal{O}_K))/2^{r_1}\pi^{r_2}$. For $\lambda = (\lambda_1, \dots, \lambda_r \in \mathbb{R}^r_{>0})$ define $\lambda_{r_1+r_2} = \lambda_{r+1} > 0$ by the formula:

$$\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$$

IN $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ consider the set:

$$B_\lambda = \{(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2} \mid |y_i| \leq \lambda_i,\ |z_j| \leq \lambda_{r_1+j})\}$$

which is a product of intervals and discs, compact, convex and centrally symmetric. Now e have that:

$$\mathrm{vol}(B_\lambda) = \prod_{i=1}^{r_1} 2\lambda_i \prod_{i=r_1+1}^{r_1+r_2} \pi\lambda_i^2 = 2^{r_1}\pi^{r_2}\alpha > 2^n \mathrm{vol}(\sigma(\mathcal{O}_K))$$

Then by Minkowski's theorem we get that there exists some $0 \neq x_\lambda \in \mathcal{O}_K$ with $\sigma(x_\lambda) \in B_\lambda$ i.e. :

$$|\sigma_i(x_\lambda)| \leq \lambda_i \qquad \text{for } 1 \leq i \leq n$$

where $\lambda_{j+r_2} := \lambda_j$ for $j = r_1 + 1, \dots, r_1 + r_2$. Since $0 \neq x_\lambda \in \mathcal{O}_K$ we have $N_{K/\mathbb{Q}}(x_\lambda)\mathbb{Z} \setminus 0$ and hence:

$$1 \leq |N_{K/\mathbb{Q}}(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{n} \lambda_i = \prod_{i1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$$

And thus:

$$|\sigma_i|(x_\lambda) = |N_{K/Q}(x_\lambda)| \prod_{j\neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{j\neq i} \lambda_j^{-1} = \frac{\lambda_i}{\alpha}$$

so we see that:

$$\frac{\lambda_i}{\alpha} \leq |\sigma_i(x_\lambda)| \leq \lambda_i$$

This implies the inequalities:

$$0 \le \log(\lambda_i) - \log(|\sigma_i(x_\lambda)|) \le \log(\alpha)$$

and hence:

$$\begin{aligned} &|\phi(L(x_\lambda)) - \sum_{i=1}^{r} c_i \log(\lambda_i)| \\ &= |\sum_{i=1}^{r} c_i (\log|\sigma_i(x_\lambda)| - \log(\lambda_i)| \\ &\le \sum_{i=1}^{r} |c_i| \log(\alpha) < \beta \end{aligned}$$

For some $\beta > 0$ which is independent of $\lambda \in \mathbb{R}^r_{>0}$ For every $\nu \in \mathbb{Z}_{\ge 1}$ choose real numbers:

$$\lambda_1^{(\nu)}, \dots \lambda_r^{(\nu)} > 0$$

such that:

$$\sum_{i=1}^{r} c_i \log(\lambda_i^{(\nu)}) = 2\nu\beta$$

and set $\lambda^{(\nu)} = (\lambda_1^{(\nu)}, \dots, \lambda_r^{(\nu)}) in \mathbb{R}^r_{>0}$ and let $x^{(\nu)} \in \mathcal{O}_K \setminus \{0\}$ as above. Then:

$$|\phi(L(x^{(\nu)}) - 2\nu\beta)| < \beta$$

and hence:

$$(2\nu - 1)\beta < \phi(L(x^{(\nu)})) < (2\nu + 1)\beta$$

In particular, for all $\nu \ge 1$ the numbers $\phi(L(x^{(\nu)}))$ are pairwise different. The estimate:

$$N(x^{(\nu)}) = |N_{K/\mathbb{Q}}(x^{(\nu)})| \le \alpha$$

shows that there are only finitely many ideals of the form $(x^{(\nu)})$. (In the proof of the finiteness of the class number we showed that there are only finitely many ideals $\alpha \in \mathcal{O}_K$ with $N(\mathfrak{a}) \le C$ for any constant C). Hence there exists $1 \le \nu < \mu$ such that:

$$(x^{(\nu)}) = (x^{(\mu)})$$

and therefore there is a unit $u \in \mathcal{O}_K^\times$ with $x^{*\mu} = ux^{(\nu)}$. Finally we find that:

$$\phi(L(u)) = \phi(L(x^{(\mu)})) - \phi(L(x^{(\nu)})) \ne 0$$

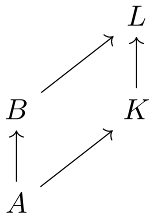
proving Claim 3* □

And hence the theorem is proven.

□

4 Decomposition Laws

Consider the following situation:



Where A is a Dedekind Domain with quotient field K, L/K a finite field extension and B the integral closure of A in L.

Proposition 4.1. *In this situation B is a Dedekind domain which is finitely generated as an A-module*

Proof. Omitted, since in our application we have that $\mathcal{O}_K = A$, $B = \mathcal{O}_L$ and the assertions are known $\square$

For a prime ideal $\mathfrak{Q} \neq 0$ in A consider the ideal $\mathfrak{Q}B$. Since B is a Dedekind domain we have that:

$$\mathfrak{Q}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

for pairwise different prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_\mathfrak{r}$ in B and $e_i \geq 1$. We want to study this decomposition.

Corollary 4.2. *For a Noetherian integral domain A every localization $S^{-1}A$ is Noetherian.*

Proposition 4.3. *R an integral domain, $A \subseteq R$ a subring. Let B be the integral closure of A in R and $S \subseteq A$ a multiplicative subset. Then $S^{-1}B$ is the integral closure of $S^{-1}A$ in $S^{-1}R$.*

Proof. For $x \in S^{-1}B$ write $x = \frac{b}{s}$ with $b \in B$ and $s \in S$. We can find $a_i \in A$ such that:

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

dividing by s^n gives:

$$(b/s)^n + a_{n-1}/s(b/s)^{n-1} + \cdots + a_0/s = 0$$

and hence $x = b/s$ is integral over $S^{-1}A$
Conversely if $y = r/s \in S^{-1}R$ with $y \in R$, $s \in S$ is integral over $S^{-1}A$, we have:

$$(r/s)^n + a_{n-1}/s_{n-1}(r/s)^{n-1} + \cdots + a_0/s_0 = 0$$

for some $a_i \in A$ and $s_i \in S$. Multiplying with $(ss_0 \cdots s_{n-1})^n$ shows that $rs_0 \cdots s_{n-1}$ is integral over A, and hence it is in B. Thus:

$$y = \frac{r}{s} = \frac{rs_0 \cdots s_{n-1}}{ss_0 \cdots s_{n-1}} \in S^{-1}B$$

$\square$

Taking $R = K = \mathrm{Quot}(A)$ we get:

Corollary 4.4. *If A is integrally closed then every localization $S^{-1}A$ is also integrally closed.*

Putting everything together we get:

Corollary 4.5. *If A is a Dedekind ring then every localization $S^{-1}A$ is also a Dedekind ring.*

The following result sometimes allows us to reduce questions about Dedekind rings to questions about principal ideal domains.

Corollary 4.6. *Let A be a Dedekind Ring, $\mathfrak{P} \neq 0$ a prime and $S = A \setminus \mathfrak{P}$. The localization $A_{\mathfrak{P}} := S^{-1}A$ is a PID which has only one non-zero prime ideal given by $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$. Any element $\pi \in A_{\mathfrak{P}}$ which $\mathfrak{m} = (\pi)$ is a prime element. The nonzero ideals $\mathfrak{a}$ of $A_{\mathfrak{P}}$ have the form $\mathfrak{a} = \mathfrak{P}^m = (\pi^m)$ for some uniquely determined $n \geq 0$.*

The next proposition concerns the behavior of localization with respect to quotients (They commute).
we now return to the situation A, B, K, L above.
For a prime ideal $\mathfrak{p}$ in A consider the prime decomposition:

$$(*) \quad \mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

Fact: The $\mathfrak{P}_i$'s are exactly the prime ideals in B "lying above" $\mathfrak{p}$ i.e. with $\mathfrak{P}_i \cap A = \mathfrak{p}$

Proof. Indeed if $\mathfrak{P} \subseteq \mathfrak{p}B$ then $\mathfrak{p} \subseteq \mathfrak{p}B \cap A \subseteq \mathfrak{P} \cap A$. Then since $\mathfrak{P} \cap A \neq A$ and $\mathfrak{p}$ is maximal we have $\mathfrak{p} = \mathfrak{P} \cap A$. Conversely if $\mathfrak{P} \cap A = \mathfrak{p}$ then $\mathfrak{p} \subseteq \mathfrak{P}$ hence $\mathfrak{p}B \subseteq \mathfrak{P}$ and the claim follows. □

Convention: One usually writes $\mathfrak{P} \mid \mathfrak{p}$ in this case.
We now introduce an important invariant for non-zero prime ideals $\mathfrak{P} \mid \mathfrak{p}$:
The inclusion $A \to B$ induces a field extension:

$$A/\mathfrak{p} \to B/\mathfrak{P}$$

and a map:

$$A/\mathfrak{p} \to B/\mathfrak{p}B$$

Since B is a finitely generated A-module $B/\mathfrak{P}$ and $B/\mathfrak{p}B$ are finite dimensional $A/\mathfrak{p}$-vector spaces.

Definition 4.7. We call:

$$f = f(\mathfrak{P}/\mathfrak{p}) := \dim_{A/\mathfrak{p}} B/\mathfrak{P}$$

the *inertia degree* of $\mathfrak{P}$ over $\mathfrak{p}$. In the decomposition $(*)$ we set $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. The exponent $e_i = e(\mathfrak{P}_\mathrm{i}/\mathfrak{p})$ is called the *ramification index* of $\mathfrak{P}_i/\mathfrak{p}$.

Theorem 4.8. (Degree formula) *With the above notation we have:*

$$\deg(L/K) = \dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \sum_{i=1}^{r} e_i f_i$$

Proof. We begin with the second equality. Writing:

$$\mathfrak{p}B = \mathfrak{q}_1 \dots \mathfrak{q}_s$$

with prime ideals $\mathfrak{q}_j$ of B we have to show that:

$$\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \sum_{j=1}^{s} = f(\mathfrak{q}_j \mid \mathfrak{p})$$

Consider the inclusions:

$$\mathfrak{p}B = \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \cdots \subset \mathfrak{q}_1\mathfrak{q}_2 \subset \mathfrak{q}_1 \subset B$$

give short exact sequences of $A/\mathfrak{P}$-vector spaces:

$$0 \to \mathfrak{a}/\mathfrak{a}\mathfrak{q}_j \to B/\mathfrak{q}_1 \cdots \mathfrak{q}_j \to B/\mathfrak{q}_1 \cdots \mathfrak{q}_{j-1} \to 0$$

where $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_{j-1}$. Thus we get:

$$\dim(B/\mathfrak{q}_1 \cdots \mathfrak{q}_j) = \dim(B/\mathfrak{q}_1 \cdots \mathfrak{q}_{\mathrm{j}-1}) + \dim(\mathfrak{a}/\mathfrak{a}\mathfrak{q}_j)$$

As a $B/\mathfrak{q}_j$-vector space $\mathfrak{a}/\mathfrak{a}\mathfrak{q}_j$ is 1-dimensional (c.f. the argument that the norm is multiplicative: There are no proper ideals between $\mathfrak{a}\mathfrak{q}_j \subset \mathfrak{a}$). Hence $\mathfrak{a}/\mathfrak{a}\mathfrak{q}_j \cong B/\mathfrak{q}_j$ has dimensions $f(\mathfrak{q}_j \mid \mathfrak{p})$ as an $A/\mathfrak{p}$-vector space. Thus:

$$\dim(B/\mathfrak{q}_1 \cdots \mathfrak{q}_j) = \dim(B/\mathfrak{q}_1 \cdots \mathfrak{q}_{j-1}) + f(\mathfrak{q}_j \mid \mathfrak{p})$$

Hence the first claim follows inductively.
Set $n = \deg(L/K)$. It remains to show that :

$$\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = n$$

First assume that A is a principal ideal domain. Then the finitely generated, torsion free A-module B is a free module of rank n. Let $x_1, \ldots, x_n$ be an A-basis of B. Then $\bar{x}_1, \ldots, \bar{x}_n$ where $\bar{x}_i = x_i + \mathfrak{p}B$ is and $A/\mathfrak{p}$-basis of $B/\mathfrak{p}B$. Indeed: Clearly these generate $B/\mathfrak{p}B$. Moreover since A is a PID we have $\mathfrak{p} = (\pi)$ for some $\pi \in A$. Assume that:

$$\sum_{i=1}^{n} \bar{\lambda}_i \bar{x}_i = 0$$

for certain $\bar{\lambda}_i \in A/\mathfrak{p}$. Thus:

$$\sum_{i=1}^{n} \lambda_i x_i = \pi b \quad \text{for some} \quad b \in B$$

moreover we can write:

$$b = \sum_{i=1}^{n} \mu_i x_i \quad \text{for} \quad \mu_i \in A$$

and hence:

$$\sum_{i=1}^{n} (\lambda_i - \pi\mu_i) x_i = 0 \in B$$

so since the x_i were a basis $\lambda_i - \pi\mu_i = 0$ and thus:

$$\bar{\lambda}_i = \bar{\pi}\bar{\mu}_i = 0 \in A/\mathfrak{p}$$

So the $\bar{x}_i$ form a basis as well. Hence we've shown that:

$$\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = n$$

Now let A be a general Dedekind Ring, then we reduce to the PID case by localizing: Let $S = A \setminus \mathfrak{p}$ and consider:

$$A_\mathfrak{p} := S^{-1}A \quad \text{and} \quad B_\mathfrak{p} := S^{-1}B$$

Then $A_\mathfrak{p}$ is a PID with quotient field K and integral closure $B_\mathfrak{p}$ in L. Since $\mathfrak{p}A_\mathfrak{p}$ is the unique non-zero prime ideal of $A_\mathfrak{p}$, we have seen that:

$$\dim_{A_{\mathfrak{p}/\mathfrak{p}}} (B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}) = n$$

Furthermore we know that the inclusion $A \hookrightarrow A_\mathfrak{p}$ induces an isomorphism:

$$A/\mathfrak{p} \xrightarrow{\sim} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$$

Hence it suffices to show that the inclusion $B \hookrightarrow B_\mathfrak{p}$ induces an isomorphism of $A/\mathfrak{p}$-vector spaces:

$$\varphi : B/\mathfrak{p}B \xrightarrow{\sim} B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$$

Clear: φ is an $A/\mathfrak{p}$-linear map.
Injectivity: We have to show that $\mathfrak{p}B_\mathfrak{p} \cap B = \mathfrak{p}B$. Need to show "$\subset$". Indeed for $c \in B$ with $c \in \mathfrak{p}B_\mathfrak{p}$

we can write $c = \frac{x}{s}$ with $x \in \mathfrak{p}B, s \in S = A \setminus \mathfrak{p}$. Since $s \in A, s \notin \mathfrak{p}$ we have $(s) + \mathfrak{p} = A$, hence there exists some $a \in A, p_1 \in \mathfrak{p}$ with:

$$sa + p_1 = 1$$

and thus:

$$(*) \quad c = csa + cp_1$$

and so:

$$c = \frac{x}{s} sa + cp_1 = xa + cp_1 \in \mathfrak{p}B$$

Surjectivity: Consider $y = \frac{c}{s} \in B_{\mathfrak{P}}, c \in B, s \in S$. Using $*$ we get:

$$y = \frac{csa}{s} + \frac{cp_1}{s} = ca + p_1 \frac{c}{s} \equiv ca \mod \mathfrak{p}B_{\mathfrak{p}}$$

Thus $y \mod \mathfrak{p}B_{\mathfrak{p}} = \varphi(ca \mod \mathfrak{p}B)$ is in the image of φ and hence φ is surjective. □

Example 4.9. Let $K/\mathbb{Q}$ be a quadratic extension, p a prime number then:

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

Since $\sum_{i=1}^{r} f_i e_i = \deg(K/Q) = 2$ we have three possibilities:

1. $r = 1, f_1 = 1, e_1 = 2$ then p is called *ramified* $p\mathcal{O}_K = \mathfrak{P}^2$
2. $r - 1 f_1 = 2, e_1 = 2$ then p is called *inert* and $p\mathcal{O}_K = p$ $r = 2, f_1 = f_2 = 1, e_1 = e_2 = 1$ the p is called *decomposed* with:

$$p\mathcal{O}_K = \mathfrak{P}_1 \mathfrak{P}_2, \ \mathfrak{P}_1 \neq \mathfrak{P}_2$$

Example 4.10. for $N \geq$ let μ_N be the group of N-th roots of unity in an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. Then μ_N is a finite subgroup of $\bar{Q}^\times$ and hence cyclic (or order N). A generator ζ of μ_N is called a primitive N-th root of unity. It induces an isomorphism $\mathbb{Z}/N \xrightarrow{\sim} \mu_N$. The primitive roots of unity in μ_n correspond to $(\mathbb{Z}/N)^\times$. Hence there are $\phi(N) := |(\mathbb{Z}/N)^\times|$ primitive N-th roots of unity in $\bar{\mathbb{Q}}$. Now let p be a prime number, $n \geq 1$ and consider $N = p^n$. In this case:

$$e := \phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

The primitive p^n-th roots of unity are the roots of the *cyclotomic* polynomial:

$$\begin{aligned} F(X) = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} &= X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \cdots + 1 \\ &= \prod_{k \in (\mathbb{Z}/p^n)^\times} (X - \zeta^k) \end{aligned}$$

where ζ is a chosen p^n-th root of unity. We have $F(1) = p$ and hence:

$$p = \prod_{k \in (\mathbb{Z}/p)^\times} (1 - \zeta^k) = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta)$$

Let B be the ring of integers of $\mathbb{Q}(\zeta)$. We have $\mu_{p^n} \subseteq B$ and hence $1 - \zeta^k \in B$ for all k.
Claim: $(1 - \zeta^i)B = (1 - \zeta^j)B$ for all $i, j \in (\mathbb{Z}/p^n)^\times$
Indeed, let $k = ij^{-1}$ in $(\mathbb{Z}/p^n)^\times$, then:

$$1 - \zeta^i = 1 - (\zeta^j)^k = (1 - \zeta^j)(1 + \zeta^j + \cdots + (\zeta^j))^{\tilde{k}-1}$$

where $\tilde{k} \in \mathbb{Z}$ is a lift of k. Therefore we get:

$$1 - \zeta^i \in (1 - \zeta^j)B \implies (1 - \zeta^i)B \subseteq (1 - \zeta^j)B$$

the claim follows by interchanging i and j. Hence we get:

$$pB = (1-\zeta)^e B = ((1-\zeta)B)^e$$

consider the prime ideal decomposition:

$$pB = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

It follows that $e \mid e_i$ for all i. Hence $e = \phi(p^n) = \deg(\mathbb{Q}(\zeta)/Q) = \sum_{i=1}^r e_i f_i \geq re$ It follows that $\mathfrak{P} = (1-\zeta)B$ is a prime ideal of B of inertia degree 1 and the decomposition of pB in B is:

$$Bp = \mathfrak{P}^e = (1-\zeta)^e \ , \ e = \phi(p^n)$$

(p is totally ramified in $\mathbb{Q}(\zeta_{p^n})$)

Remark 4.11. We will see later that $B = \mathbb{Z}[\zeta_{p^n}]$

We now give an explicit method to determine the prime ideal decomposition explicitly in our usual K, L, A, B situation $\mathfrak{p}$ a prime ideal in A where L/K is separable and $L = K[\theta]$ with $\theta \in B$. Let $P(X)$ be the minimal polynomial of θ over K. We know that:

$$P(X) \in A[X]$$

The method will apply to all prime ideals $\mathfrak{p}$ of A which are prime to the so called *conductor* f of the subring $A[\theta]$ in B. The conductor is by definition the biggest ideal of B which is contained in $A[\theta]$. Explicitly:

$$f = \{\alpha \in B \mid \alpha B \subseteq A[\theta]\}$$

Note: If $B = A[\theta]$ then $f = (1) = B$ and then our method will apply Ci all $\mathfrak{p}$.
Here's the method:

Theorem 4.12. *Let $\mathfrak{p} \neq 0$ be a nonzero prime ideal of A with $\mathfrak{p} \nmid f \cap A$. Let:*

$$\bar{P}(X) = \bar{P}_1(X)^{e_1} \cdots \bar{P}_r(X)^{e_r}$$

be the decomposition of:

$$\bar{P}(x) := P(X) \mod \mathfrak{p} \in A/\mathfrak{p}[X]$$

into a product of monic irreducible factors which are pairwise different. Choose monic polynomials $P_i(X) \in A[X]$ with:

$$\bar{P}_i(X) = P_i(X) \mod \mathfrak{p}$$

Then $\mathfrak{P}_i = \mathfrak{p}B + P_i(\theta)B \quad$ for $1 \leq i \leq r$ are the r pairwise different prime ideals in B lying over $\mathfrak{p}$. Moreover we have:

$$f_i = f(\mathfrak{P}_i \mid \mathfrak{p}) = \deg \bar{P}_i(X)$$

and:

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

Without knowing B explicitly it is difficult to determine f. However we have the following information:

Lemma 4.13. *In the situation of the theorem let $d_\theta = d(1, \theta, \ldots, \theta^{n-1}) \in A$ beg the discriminant of the basis $1, \theta, \ldots, \theta^{n-1}$ of $L = K(\theta)$, then $f \mid d_\theta B$. In particular, for all prime ideals $\mathfrak{p}$ of A with $\mathfrak{p} \nmid (d_\theta)$ we have $\mathfrak{p} \nmid f \cap A$*

Proof. We have already shown that we have an inclusion:

$$d_\theta B \subseteq A + \theta A + \cdots + \theta^{n-1} A = A[\theta]$$

Hence $d_\theta \in f$ i.e. $f \mid d_\theta B$. we have inclusions:

$$(d_\theta) = d_\theta A \subseteq d_\theta B \cap A \subseteq f \cap A$$

Thus if $\mathfrak{p} \nmid (d_\theta)$ we have $\mathfrak{p} \nmid f \cap A$ as claimed. □

Example 4.14. $A = \mathbb{Z}, K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}), B = \mathcal{O}_L$ choose $\theta = \sqrt[r]{2} \in B$. Then $P(X) = X^3 - 2$, we've seen that:

$$d_\theta = -108 = -2^2 \cdot 3^3$$

Hence all prime ideals $\mathfrak{p} = p\mathbb{Z}$ for $p \neq 2, 3$ are prime to the conductor f of $\mathbb{Z}[\theta]$

1. For $p = 7$ we have:

$$\bar{P}(X) = X^3 - \bar{2} \in \mathbb{F}_7[X]$$

   which is irreducible since there are no third roots of $2 \in \mathbb{F}_7$. Thus $r = 1, e_1 = 1, f_1 = \deg(\bar{P}(X) = 3)$

$$\mathfrak{P} = 7\mathcal{O}_L + P(\theta)\mathcal{O}_L = 7\mathcal{O}_L$$

   so $7\mathcal{O}_L$ is prime and $\mathcal{O}_L/\mathfrak{P} = \mathbb{F}_{7^3}$

2. For $p = 11$ the polynomial:

$$\bar{P}(X) = X^3 - \bar{2} \in \mathbb{F}_{11}[X]$$

   has a root, namely $-\bar{4}$. Hence:

$$X^3 - \bar{2} = (X + \bar{4})(X^2 + aX + b)$$

   One finds that $a = -\bar{4}$ and $b = \bar{5}$ hence:

$$X^3 - \bar{2} = (X + \bar{4})(X^2 - \bar{4}X + \bar{5})$$

   Where the second factor is irreducible since it has no roots in $\mathbb{F}_{11}$ Thus $r = 2$ and:

$$11\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$$

   where:

$$\mathfrak{P}_1 = (11, \sqrt[3]{2} + 4), \ f_1 = 1$$
$$\mathfrak{P}_2 = (11, \sqrt[3]{4} - 4\sqrt[4]{2} + 5), \ f_2 = 2$$

For the proof of our theorem we need the following:

Lemma 4.15. *Let $R = \prod_{i=1}^n R_i$ be a ring, then the prime ideas $\mathfrak{q}$ of R have the form:*

$$\mathfrak{q} = R_1 \times \cdots \times \mathfrak{q}_i \times \cdots \times R_n = \pi_i^{-1}(\mathfrak{q}_i)$$

for some i and some prime ideal $\mathfrak{q}_i$ of R_i. Here $\pi_i : R \to R_i$ is the projection. It induces an isomorphism:

$$R/\mathfrak{q} \xrightarrow{\sim} R_i/\mathfrak{q}_i$$

Proof of the Theorem. Let $\mathfrak{p} \nmid f \cap A$ be a prime ideal as in the theorem.

<u>Claim 1</u>: The inclusion $C = A[\theta] \hookrightarrow B$ induces an isomorphism:

$$(*) \quad C/\mathfrak{p}C \xrightarrow{\sim} B/\mathfrak{p}B$$

Proof. If a prime ideal $\mathfrak{P}$ of B divides $\mathfrak{p}B$ and f then:

$$\mathfrak{p} = \mathfrak{P} \cap A \mid f \cap A$$

which is a contradiction. Hence $\mathfrak{p}B$ and f are coprime, i.e. $\mathfrak{p}B + f = B$. By definition we have $f \subseteq C$ and therefore $\mathfrak{p}B + C = B$. Thus the canonical map $C \to B/\mathfrak{p}B$ is surjective. Its kernel is $\mathfrak{p}B \cap C$ and for injectivity of $(*)$ it remains to show that $\mathfrak{p}B \cap C = \mathfrak{p}C$. Only need to show "$\subseteq$": By $\mathfrak{p} \nmid f \cap A$ we know that $\mathfrak{p} + (f \cap A) = A$ (since $\mathfrak{p}$ is maximal). Hence $A \subseteq \mathfrak{p} + f$ and therefore:

$$\mathfrak{p}B \cap C \subseteq (\mathfrak{p} + g)(\mathfrak{p}B \cap C) \subseteq \mathfrak{p}C + \mathfrak{p}fB \subseteq \mathfrak{p}C$$

Where the last inclusion holds since $fB \subseteq f \subseteq C$. □

The projection $A \to \bar{A} = A/\mathfrak{p}$ induces surjective ring maps:

$$A[X] \to \bar{A}[X] = A[X]/\mathfrak{p}(X),\ Q \mapsto \bar{Q}$$

$$A[X]/P(X) \to \bar{A}[X]/(\bar{P}(X))$$

Claim 2: The surjective composition:

$$C = A[\theta] \xrightarrow{\sim} A[X]/P(X) \to \bar{A}[X]/\bar{P}(X)$$

induces an isomorphism:

$$C/\mathfrak{p}C \xrightarrow{\sim} \bar{A}[X]/\bar{P}(X)$$

Proof. The kernel consists of those elements $\bar{Q}(X) in (\bar{P}(X))$ which is equivalent to $\bar{Q}(X) = \bar{P}(X) = \bar{S}(X)$ for some $\bar{S} \in \bar{A}[X]$ i.e. $Q(X) = P(X)S(X) + T(X)$ for some $S \in A[X]$ and $T \in \mathfrak{p}(X)$ i.e. $Q(\theta) = T(\theta)$ for some $T \in \mathfrak{p}(X)$ i.e. $Q(\theta) \in \mathfrak{p}(\theta) = \mathfrak{p}C$ □

By these two claims the following map is an isomorphism:

$$\bar{A}[X]/\bar{P}(X) \xrightarrow{\sim} B/\mathfrak{p}B$$

$$\bar{Q} \mod \bar{P}(X) \mapsto Q(\theta) \mod \mathfrak{p}B$$

The Chinese remainder theorem gives an isomorphism:

$$R := \bar{A}[X]/\bar{P}(X) \xrightarrow{\sim} \prod_{i=1}^{r} \bar{A}[X]/\bar{p}_i(X)^{e_i}$$

Now let $\mathfrak{q}_i$ be a prime ideal of $R_i = \bar{A}[X]/\bar{P}_i(X)^{e_i}$. Its inverse image in $\bar{A}[X]$ is a prime ideal $\tilde{\mathfrak{q}}_i$ which contains $(\bar{P}_i(X)^{e_i})$. It follows that in fact $\bar{P}_i(X) \subseteq \tilde{\mathfrak{q}}_i$ and hence $\tilde{\mathfrak{q}}_\mathrm{i} = (\bar{P}_i(X))$ since $\bar{P}_i(X)$ is maximal in $\bar{A}[X]$. Thus R_i has a unique prime ideal:

$$\mathfrak{q}_i = (\bar{P}_i(X) \bmod (\bar{P}_i(X)^{e_i}))$$

Its inverse image in R is the prime ideal (π_i) where:

$$\pi_i = \bar{P}_i(X) \bmod (\bar{P}(X))$$

Now using our Lemma we get the following:

(a) The prime ideals of R are the ideals (π_i)

(b) $R/(\pi_i) \xrightarrow{\sim} \bar{A}[X]/\bar{P}_i(X)$ and in particular:

$$\dim_{\bar{A}} R/(\pi_i) = \deg \bar{P}_i(X)$$

(c) $\bigcap_{i=1}^{r}(\pi_i^{e_i}) = 0$

Using the above isomorphism:

$$R = \bar{A}[X]/\bar{P}(X) \xrightarrow{\sim} B/\mathfrak{p}B$$

$$\bar{Q} \bmod \bar{P}(X) \mapsto Q(\theta) \bmod \mathfrak{p}B$$

we get:

1. The prime ideals of $\bar{B} := B/\mathfrak{p}B$ are the principle ideals $\bar{\mathfrak{P}}_i = (\overline{P_i(\theta)})$ where $\overline{P_i(\theta)} := P_i(\theta) \bmod \mathfrak{p}B \in \bar{B}$
2. $\dim_{\bar{A}} \bar{B}/\bar{\mathfrak{P}}_i = \deg \bar{P}_i(X)$

3. $\bigcap_{i=1}^r \bar{\mathfrak{P}}_i^{e_i} = 0$

The inverse image of $\bar{\mathfrak{P}}_i$ under the projection $B \to \bar{B}/\mathfrak{p}B$ is the prime ideal:

$$\mathfrak{P}_i = \mathfrak{p}B + P_i(\theta)B$$

where $P_i \in A[X]$ is any polynomial lifting $\bar{P}_i$. The (prime) ideals of $\bar{B}$ correspond bijectively to the (prime) ideals of B which contain $\mathfrak{p}B$ hence:

1. The $\mathfrak{P}_i$'s are exactly the pairwise different prime ideals lying over $\mathfrak{p}$.
2. $f_i = \dim_{A/\mathfrak{p}} B/\mathfrak{P}_i = \dim_{\bar{A}} \bar{B}/\mathfrak{P}_i = \deg \bar{P}_i(X)$
3. $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$

(Still need to do some work for the last statement, I was too tired) □

Special cases of the decomposition of a prime:

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

Let $n = \deg(L/K)$ then:

$$\sum_{i=1}^{r} e_i f_i = n$$

1. If $r = n$ i.e. $e_i = f_i = 1$ for all i then $\mathfrak{p}$ is called *completely decomposed* in B (L)
2. The prime ideal $\mathfrak{P}_{\mathfrak{i}}$ is called *unramified* if $e_i = 1$ and if the field extension:

   $$A/\mathfrak{p} \to B/\mathfrak{P}_i$$

   is separable (For extensions of number fields $A = \mathcal{O}_K$, $B = \mathcal{O}_L$ is always satisfied since the quotients are finite.)
3. If $e_i > 1$ then $\mathfrak{P}_i$ is called *ramified* and if additionally $f_i = 1$ then it is called *purely ramified.*
4. $\mathfrak{p}_i$ is called *unramified* if all the $\mathfrak{P}_i$ are unramified. Otherwise $\mathfrak{p}$ is called *ramified* and one says that "$\mathfrak{p}$ ramifies in B"

We have that:

Theorem 4.16. *If L/K is separable then only finitely many prime ideals $\mathfrak{p}$ of A ramify in B.*

Proof. Since L/K is finite and separable we can find some $\theta \in \mathcal{O}_L$ such that $L = K[\theta]$. Now let $P(X)$ be the minimal polynomial of θ and $d_\theta \in A$ the discriminant of the basis $1, \theta, \ldots, \theta^{n-1}$. Let $\widetilde{L}$ be the Galois closure of L/K. There are n pairwise different embeddings $\sigma_i : L \hookrightarrow \widetilde{L}$ over K and the images $\theta_i = \sigma_i(\theta) \in \widetilde{L}$ are pairwise different. Let $\widetilde{B}$ be the integral closure of A in $\widetilde{L}$. Then $B \subseteq \widetilde{B}$ and $\theta_i \in \widetilde{B}$ for all i. Hence we get a factorization:

$$P(X) = \prod_{i=1}^{n} (X - \theta_i) \in \widetilde{B}[X]$$

and moreover:

$$d_\theta = \prod_{i<j} (\theta_i - \theta_j)^2 \in A$$

choose a prime ideal $\widetilde{\mathfrak{P}}$ of $\widetilde{B}$ over $\mathfrak{p}$. then the polynomial:

$$\bar{P}(X) \in A/\mathfrak{p}[X]$$

decomposes into linear factors in the extension field $\widetilde{B}/\widetilde{\mathfrak{P}}$ of $A/\mathfrak{p}$ namely:

$$\bar{P}(X) = \prod_{i=1}^{n}(X - \bar{\theta}_i) \in \widetilde{B}/\widetilde{\mathfrak{P}}[X]$$

We have:

$$\bar{d}_\theta = d_\theta \bmod \mathfrak{p} = \prod_{i<j}(\bar{\theta}_i - \bar{\theta}_j)^2 \in A/\mathfrak{p}$$

Claim: If $\mathfrak{p} \nmid (d_\theta)$ then $\mathfrak{p}$ is unramified in B.

Indeed. Since $\mathfrak{p} \nmid (d_\theta)$ we know how to compute the prime ideal decomposition of $\mathfrak{p}B$. in the decomposition of $\bar{P}(X) \in A/\mathfrak{p}[X]$ into irreducible factors:

$$\bar{P}(X) = \bar{P}_1(x)^{e_1} \cdots \bar{P}_r(X)^{e_r}$$

all $e_i = 1$ since $\mathfrak{p} \nmid (d_\theta) \implies \bar{d}_\theta \neq 0 \in A/\mathfrak{p}$ and hence the $\bar{\theta}_i \in \widetilde{B}/\widetilde{\mathfrak{P}}$ are pairwise different. Hence $\bar{P}(X)$ decomposes into pairwise different linear factors over $\widetilde{B}/\widetilde{\mathfrak{p}}$ and hence:

$$\mathfrak{p}B = \mathfrak{P}_1 \cdots \mathfrak{P}_r, \quad \text{i.e. } e_i = 1$$

□

Fix $\mathfrak{P}_i$ over $\mathfrak{p}$ and let $\bar{\theta} = \theta \bmod \mathfrak{P}_i$ in $B/\mathfrak{P}_i$. The above argument for some $\widetilde{\mathfrak{P}}$ over $\mathfrak{P}_i$ shows that $\bar{\theta}$ is a zero of a polynomial over $A/\mathfrak{p}$ which has only simple roots. Hence $\bar{\theta}$ is separable and therefore so is:

$$(*) \quad A/\mathfrak{p}[\theta] = B/\mathfrak{P}_i$$

Indeed consider the composition:

$$A[\theta] \hookrightarrow B \to B/\mathfrak{P}_i$$

since $\mathfrak{p} \nmid (d_\theta) \implies \mathfrak{p} \nmid f$ and therefore $A[\theta] + \mathfrak{p}B = B$ and thus $A[\theta] + \mathfrak{P}_i = B$, so this map is surjective. Thus the equality $(*)$ holds and we are done. □

We have the following more precises assertion:

Theorem 4.17. *(a) Let $\mathcal{D}$ be the ideal of A which is generated by the discriminants of all bases of L/K contained in B. Then a prime $\mathfrak{p}$ of A ramified in B if and only if $\mathfrak{p} \mid \mathcal{D}$*

(b) For $A = Z$, $K = \mathbb{Q}$ and a number field $L\mathbb{Q}$ the prime ideal $(p) = p\mathbb{Z}$ ramifies in $\mathcal{O}_L$ if and only if $p \mid d_{L/\mathbb{Q}}$

Assertion (b) is a special case of (a) because $\mathcal{O}_L$ is a free $\mathbb{Z}$-module and hence $\mathcal{D} = (d_{L/\mathbb{Q}})$

Proof. Omitted □

Corollary 4.18. *Let $L \neq \mathbb{Q}$ be a number field, then there is at least one prime number p such that (p) is ramified in $\mathcal{O}_L$.*

Proof. We've seen that $|d_{L/\mathbb{Q}}| \geq 2$ and hence $d_{L/\mathbb{Q}}$ has a prime divisor p. Then by our theorem p ramified in L. □

5 Decomposition Laws in Quadratic Fields

$K/\mathbb{Q}$ quadratic field there exists $d \in \mathbb{Z}, d \neq 1$ d not divided by a square with $\mathbb{Q}(\sqrt{d})$. The discriminant is:

$$\mathcal{D} = \begin{cases} 4d, & d \not\equiv 1 \bmod 4 \\ d, & d \equiv 1 \bmod 4 \end{cases}$$

Set $\theta = \frac{D+\sqrt{D}}{2}$ then we always have $\mathcal{O}_K = \mathbb{Z}[\theta]$. Moreover set $\theta' = \frac{D-\sqrt{D}}{2}$ then the minimal polynomial of θ over $\mathbb{Q}$ is given by:

$$\begin{aligned} P(X) = (X-\theta)(X-\theta') &= X^2 - Tr(\theta)X + N(\theta) \\ &= X^2 - DX + \frac{D(D-1)}{4} \in \mathbb{Z}[X] \\ &= (X - \frac{D}{2})^2 - \frac{D}{4} \in \mathbb{Q}[X] \end{aligned}$$

Since $\mathcal{O}_K = \mathbb{Z}[\theta]$ the conductor of $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$ is trivial and we can compute the decomposition of all primes $p \in \mathbb{Z}$. There are three possibilities:

1. $p\mathcal{O}_K = \mathfrak{P}^2$ ramified
2. $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$ decomposed
3. $p\mathcal{O}_K = \mathfrak{P}$ inert

Fix a prime $p \neq 2$, then $a \in \mathbb{Z}$ is called a *quadratic residue mod* p if $p \nmid a$ and a is a square in $\mathbb{Z}/p$

Theorem 5.1.

(a) p is ramified in K iff $p \mid D$

(b) p is decomposed iff either $p \neq 2$ and D (equiv d) is a quadratic residue mod p *or $p = 2$ and $D \equiv 1$* mod 8 *(or equiv d)*

(c) p is inert in K if either $p \neq 2$ and D is a quadratic non-residue mod p *or $p = 2$ and $D \equiv 5$* mod 8 *(or equivalently d)*

Proof. The assertions for d follow from those for D. We know that p is ramified if and only if $\bar{P}(X) = P(X) \bmod p \in \mathbb{F}_p[X]$ has multiple zeroes, i.e. since $D = (\theta - \theta')^2$ iff $\bar{D} = D \bmod p = 0$ i.e. $p \mid D$. Now assume that $p \nmid D$. Then p is decomposed iff $\bar{P}(X)$ decomposes into linear factors in $\mathbb{F}_p[X]$ i.e. iff $\bar{P}(X)$ has a root in $\mathbb{F}_p$:
Assume $p \neq 2$, then $2 \in \mathbb{F}_p^\times$ and hence:

$$\bar{P}(X) = (\bar{X} - \bar{D}/2)^2 - \bar{D}/4 \in \mathbb{F}_p[X]$$

thus $\bar{P}(X)$ has a root in $\mathbb{F}_p$ iff $\bar{D}/4$ (or equivalently $\bar{D}$) is a square $\mathbb{F}_p^\times$.
Now Assume $p = 2$, thus $2 \nmid D \implies D = d \equiv 1 \bmod 4$ and hence $D \equiv 1, 5 \bmod 8$. For $D \equiv 1 \bmod 8$ we have:

$$\bar{P}(X) = X^2 + X = X(X+1) \in \mathbb{F}_2[X]$$

and hence $p = 2$ is decomposed. On the other hand for $D \equiv 5 \bmod 8$ we get:

$$\bar{P}(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$$

which has no roots in $\mathbb{F}_2$. Hence $\bar{P}$ is irreducible i.e. $p = 2$ is inert. □

6 Quadratic reciprocity

Proposition 6.1. *For a prime $p \neq 2$ the subgroup:*

$$(\mathbb{F}_p^\times)^2 := \left\{x^2 \mid x \in \mathbb{F}_p^\times\right\}$$

is a subgroup of index 2 in $\mathbb{F}_p^\times$. It is the kernel of the homomorphism:

$$\left(\frac{-}{p}\right) : \mathbb{F}_p^\times \to \mu_2, \quad x \mapsto \left(\frac{x}{p}\right) := x^{\frac{p-1}{2}}$$

i.e. we have an exact sequence:

$$1 \to (\mathbb{F}_p^\times)^2 \to \mathbb{F}_p^\times \xrightarrow{\left(\frac{-}{p}\right)} \mu_2 \to 1$$

Proof. Since $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ and since p is odd this follows from the exact sequence:

$$0 \to 2\mathbb{Z}/(p-1)\mathbb{Z} \to \mathbb{Z}/(p-1)\mathbb{Z} \xrightarrow{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)\mathbb{Z}/(p-1)\mathbb{Z} \to 0$$

□

Remark 6.2. 1. $\left(\frac{x}{p}\right)$ is called the *Legendre symbol* of x over p. we set $\left(\frac{0}{p}\right) := 0$ so we have $\left(\frac{x}{p}\right) = 1 \iff x \in (\mathbb{F}_p^\times)^2$
   For $a \in \mathbb{Z}$ write:

$$\left(\frac{a}{p}\right) := \left(\frac{a \bmod p}{p}\right) \in \{\pm 1, 0\}$$

   Then $\left(\frac{a}{p}\right) = 1 \iff a$ is a quadratic residue mod p

2. $\left(\frac{-}{p}\right)$ is multiplicative.

3. For $x \in \mathbb{F}_p^\times$, if $y^2 = x$ for some $y \in \bar{\mathbb{F}}_p$ then:

$$\left(\frac{x}{p}\right) = y^{p-1}$$

   since $y^{p-1} = (y^2)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}}$

We now look at the special cases $x = 1, -1, 2 \in \mathbb{F}_p^\times$.
the following maps are homomorphisms:

$$\varepsilon : (\mathbb{Z}/4)^\times \to \mathbb{Z}/2, \quad \varepsilon(n \bmod 4) = \frac{n-1}{2} \bmod 2$$

$$\omega : (\mathbb{Z}/8)^\times \to \mathbb{Z}/2, \quad \omega(n \bmod 8) = \frac{n^2-1}{8} \bmod 2$$

Proposition 6.3. *For $p \neq 2$ we have:*

1. $\left(\frac{1}{p}\right) = 1$

2. $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$

3. $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$

Proof. (1) and (2) are clear by definition. Let ζ be a p-th primitive root of unity in $\bar{\mathbb{F}}_p$ i.e. $\zeta^8 = 1, \zeta^4 = -1$. Since $f(X) = X^n - 1$ has no multiple roots in $\bar{F_p}$. For $y = \zeta + \zeta^{-1}$ we have $y^2 = 2$. Applying the Frobenius automorphism $x \mapsto x^p$ of $\bar{\mathbb{F}}_p$ we get:

$$y^p = \zeta^p + \zeta^{-p}$$

For $p \equiv \pm 1 \mod 8$ we get $\zeta^p = \zeta^{\pm 1}$ hence $y^p = y$ hence:

$$\left(\frac{2}{p}\right) = y^{p-1} = 1 = (-1)^{\omega(p)}$$

For $p \equiv \pm \mod 8$ we get $\zeta^p = -\zeta^{\pm 1}$ and hence $y^p = -y$ so:

$$\left(\frac{2}{p}\right) = y^{p-1} = -1 = (-1)^{\omega(p)}$$

$\square$

Remark 6.4. In other words, for $p \neq 2$ -1 is a quadratic residue mod p iff $p \equiv 1 \mod 4$ and 2 is a quadratic residue mod p iff $p \equiv \pm 1 \mod 8$

Corollary 6.5. *A prime number p is of the form $p = n^2 + m^2$ with $n, m \in \mathbb{Z}$ iff $p \equiv 1 \mod 4$*

Proof. The following are equivalent: $p \equiv 1 \mod 4 \iff -1$ is a quadratic residue $\mod p \iff p$ is decomposed in $\mathbb{Q}(i)$. Let $p \equiv 1 \mod 4 \implies p$ is decomposed in $\mathbb{Q}(i)$. Thus $p\mathbb{Z}[i] = \mathfrak{p}_1\mathfrak{p}_2$ for $\mathfrak{p}_1 \neq \mathfrak{p}_2$ in $\mathbb{Z}[i]$ and hence:

$$p^2 = N(p\mathbb{Z}[i]) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)$$

hence $N(\mathfrak{p}_1) = N(\mathfrak{p}_2)$. We have $\mathfrak{p}_1 = (n + mi)$ for some $n, m \in \mathbb{Z}$. Since $\mathbb{Z}[i]$ is euclidean and hence a PID. Thus:

$$p = N(\mathfrak{p}_1) = n^2 + m^2$$

On the other hand, since $n^2 \equiv 0, 1 \mod 4$ for all n, the equality $p = n^2 + m^2$ implies that $p \equiv 0, 1, 2 \mod 4$, and since $p \neq 2$ we get that $p \equiv 1 \mod 4$ $\square$

Theorem 6.6. (Gauss' Quadratic Reciprocity Law)
For odd primes $p \neq \ell$ we have:

$$\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)(-1)^{\varepsilon(\ell)\varepsilon(p)}$$

We will give a conceptual proof later using cyclotomic fields.

Remark 6.7. The theorem can be used to calculate Legendre symbols as in the following example:

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$$

7 Hilbert Theory

In our usual situation we now assume that the extension L/K is Galois and discuss the consequences of the prime ideal decomposition.

Remark 7.1. we have that $\sigma(B) = B$ for $\sigma \in G$ since if $\mathfrak{P} \in A[X]$ is a monic polynomial, then:

$$P(b) = 0 \iff 0 = \sigma(P(b)) = P(\sigma(b))$$

For a prime ideal $\mathfrak{P}$ of B, $\sigma(\mathfrak{P})$ is again a prime ideal of B. Let $0 \neq \mathfrak{p} \subseteq A$ be a prime ideal. In:

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{p}_1^{e_r}$$

the $\mathfrak{P}_i$ are those prime ideals $\mathfrak{P}$ of B with $\mathfrak{P} \cap A = \mathfrak{p}$. Applying $\sigma \in G$ gives:

$$\mathfrak{p} = \sigma(\mathfrak{p}) = \sigma(\mathfrak{P} \cap A) = \sigma(\mathfrak{P} \cap \sigma(A)) = \sigma(\mathfrak{P} \cap A)$$

Hence:

$$\mathfrak{P} \mid \mathfrak{p}B \iff \sigma(\mathfrak{P}) \mid \mathfrak{p}B$$

and σ permutes the $\mathfrak{P}_i$. Hence the group G acts on the set $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$. Claim: We have that:

$$e(\sigma(\mathfrak{P} \mid \mathfrak{p})) = e(\mathfrak{P} \mid \mathfrak{p})$$

for $\mathfrak{P} \mid \mathfrak{p}$ and $\sigma \in G$

Proof. This is clear if $\sigma(\mathfrak{P}) = \mathfrak{P}$. Otherwise we may assume $\mathfrak{P} = \mathfrak{P}_1$ and $\sigma(\mathfrak{P}) = \mathfrak{P}_2$. Then we have:

$$\prod_{i=1}^{r} \mathfrak{P}_i^{e_i} = \mathfrak{p}B = \sigma(\mathfrak{p}B) = \prod_{i=1}^{r} \sigma(\mathfrak{P}_i^{e_i}) = \mathfrak{P}_2^{e_1} \cdots$$

□

then the uniqueness of the decomposition implies that $e_2 = e_1$

Theorem 7.2. *Let $0 \neq \mathfrak{p}$ be a prime ideal of A. Then the $\mathfrak{P} \mid \mathfrak{p}$ are pairwise conjugate and they all have the same inertia degree f and ramification index e. Thus we have:*

$$\mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e \quad \text{and} \quad \deg(L/K) = efr \tag{3}$$

Proof. It suffices to show that for $\mathfrak{P}, \mathfrak{P}' \mid \mathfrak{p}B$ we have $\mathfrak{P}' = \sigma(\mathfrak{P})$ for some $\sigma \in G$. the the iso $\sigma : B \to B$ induces an $A/\mathfrak{p}$-linear isomorphism:

$$\bar{\sigma} : B/\mathfrak{P} \xrightarrow{\sim} B/\sigma(\mathfrak{P})$$

and hence $f(\mathfrak{P} \mid \mathfrak{p}) = f(\sigma(\mathfrak{P}) \mid \mathfrak{p})$ as desired.
So given $\mathfrak{P} \mid \mathfrak{p}$ assume there exists $\mathfrak{P}' \mid \mathfrak{p}$ such that $\mathfrak{P} \neq \sigma(\mathfrak{P})$ for all $\sigma \in G$. Then $\mathfrak{P}' \not\subseteq \sigma(\mathfrak{P})$ since $\sigma(\mathfrak{P})$ is a maximal ideal. Now:

Lemma 7.3. *Let R be a ring, $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ Prime ideals of R, $\mathfrak{b}$ and ideal with $\mathfrak{b} \not\subseteq \mathfrak{p}_i$ for all i. Then there exists some $b \in \mathfrak{b}$ with $b \notin \mathfrak{p}_i$ for all i.*

By the lemma, there exists an element $x \in \mathfrak{P}'$ with $x \notin \sigma(\mathfrak{P})$ for all $\sigma \in G$. Then:

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in \mathfrak{P}$$

(Indeed, since $\sigma(x) = x$ for $\sigma = \text{id}$, for all $\sigma \in G$ we have $\sigma(x) inB$)
Hence $N_{L/K}(x) \in \mathfrak{P}' \cap A = \mathfrak{p}$. Moreover we have that $x \notin \sigma^{-1}(\mathfrak{P})$ for all $\sigma \in G$. Hence $\sigma(x) \notin \mathfrak{P}$ and thus:

$$N_{L/K}(x) \notin \mathfrak{P} \quad \text{since } \mathfrak{P} \text{ is a prime ideal}$$

$\implies N_{L/K}(x) \notin \mathfrak{p}$ which is a contradiction. □

Let $\mathfrak{p} \neq 0$ be a prime ideal of A. By our theorem the action on the set of prime ideals in B dividing $\mathfrak{p}$ is transitive. The stabilizer group of $\mathfrak{P}$ denoted $G_{\mathfrak{P}}$ is called the *decomposition* group of $\mathfrak{P}$. The map:

$$G/G_{\mathfrak{P}} \xrightarrow{\sim} \{\mathfrak{P} \mid \mathfrak{P} \mid \mathfrak{p}\}$$

$$\sigma G_{\mathfrak{P}} \mapsto \sigma(\mathfrak{P})$$

is a bijection. Hence $|G|/|G_{\mathfrak{P}}| = |G/G_{\mathfrak{P}}| = r$ and since $|G| = \deg(L/K) = efr$ we see that $|G_{\mathfrak{P}}| = ef$.
Every $\sigma \in G_{\mathfrak{P}}$ induces an $A/\mathfrak{p}$-linear isomorphism:

$$\bar{\sigma} : B/\mathfrak{P} \xrightarrow{\sim} B/\mathfrak{P}$$

Let $\mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{P})$ be the group of $a/\mathfrak{p}$-linear automorphisms of the field $B/\mathfrak{P}$. we get a homomorphism:

$$G_{\mathfrak{P}} \to \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{P}),\ \sigma \mapsto \bar{\sigma}$$

The kernel of this map is the *inertia subgroup* of $\mathfrak{P}$ denoted by $I_{\mathfrak{P}}$. By definition $I_{\mathfrak{P}}$ is a normal subgroup of $G_{\mathfrak{P}}$ and we have:

$$I_{\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}} \mid \sigma(x) - x \in \mathfrak{P} \text{ for all } x \in B\}$$

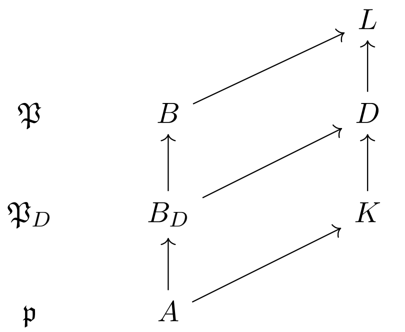
Theorem 7.4. *With notations as above, assume that the residue field extension $B/\mathfrak{P}$ is separable. Then $B/\mathfrak{P}$ is Galois of degree f over $A/\mathfrak{p}$. Moreover we have that:*

$$|I|_{\mathfrak{P}} = e$$

and there is a short exact sequence:

$$1 \to I_{\mathfrak{P}} \to G_{\mathfrak{P}} \to \mathrm{Gal}(B/\mathfrak{P}, A/\mathfrak{p}) \to 1$$

Proof. Let $D = L^{G_{\mathfrak{P}}}$ be the *decomposition field of $\mathfrak{P}$ over K*. Let $B_D = B \cap D$ be the integral closure of A in D. Set $\mathfrak{P}_D = \mathfrak{P} \cap B_D$. so we have:



By our theorem $G_{\mathfrak{P}}$ acts transitively on the prime ideals in B over $\mathfrak{P}_D$. By definition of $G_{\mathfrak{P}}$ it follows that $\mathfrak{P}$ is the only prime ideal over $\mathfrak{P}_D$. Hence for some $e' \geq 1$ we have:

$$\mathfrak{P}_D = \mathfrak{P}^{e'}$$

Let $f' = f(\mathfrak{P} \mid \mathfrak{P}_D)$, then:

$$e'f' = \deg(L/D) = |G_{\mathfrak{P}}| = ef$$

The injective homomorphisms:

$$A/\mathfrak{P} \hookrightarrow B_D/\mathfrak{P}_D \hookrightarrow B/\mathfrak{P}$$

shows that:

$$f' = \deg(B/\mathfrak{P}/B_D/\mathfrak{P}_D) \leq \deg(B/\mathfrak{P}/A\mathfrak{P}) = f$$

By $\mathfrak{P}_d \mid \mathfrak{p}$ we have $\mathfrak{P}_D = \mathfrak{P}^{e'} \mid \mathfrak{P} = \mathfrak{P}^e$ and hence $e' \leq e$. Together this shows that $e = e'$ and $f = f'$ and hence $\mathfrak{P}_D = \mathfrak{P}^e$ moreover $A/\mathfrak{p} \xrightarrow{\sim} B_D/\mathfrak{P}_D$ Since $B/\mathfrak{P}$ over $A/\mathfrak{p}$ was supposed to be separable there exists a primitive element $\bar{x} \in B/\mathfrak{P}$. Let $x \in B$ be a lift of $\bar{x}$. Let:

$$X^m + a_{m-1}X^{m-1} + \cdots + a_0$$

be the minimal polynomial of x over D. Since x is integral over B_D, the $a_i \in B_D$. Each zero of the polynomial has the form $\sigma(x)$ of some $\sigma \in \mathrm{Gal}(L/D) = G_{\mathfrak{P}}$. Reducing mod $\mathfrak{P}_D$ we get a polynomial with coefficients in $B_D/\mathfrak{P}_D = A/\mathfrak{p}$.

$$(**) \quad X^m + \bar{a}_{m-1}X^{m-1} + \cdots + \bar{a}_0 \in A/frakp$$

Its roots in $B/\mathfrak{P}$ have the form:

$$\sigma(\bar{x}) = \bar{\sigma}(\bar{x}) \in B/\mathfrak{P}$$

for $\sigma \in G_{\mathfrak{P}}$. Thus $B/\mathfrak{P}$ contains all roots of $(**)$ and the y generate $B/\mathfrak{P}$ over $A/\mathfrak{p}$. Hence $B/\mathfrak{P}$ is the decomposition field of the polynomial over $A/\mathfrak{p}$, and hence $B/\mathfrak{P}$ is normal over $a/\mathfrak{p}$ and being separable it is also Galois.

Let $\tau \in \mathrm{Gal}(B/\mathfrak{P}), A/\mathfrak{p}$, since $\tau(\bar{x})$ is a zero of $(**)$ there exists $\sigma \in G_{\mathfrak{P}}$ such that $\bar{\sigma}(\bar{x}) = \tau(\bar{x})$. Since $\bar{x}$ is a primitive element it follows that $\bar{\sigma} = \tau$. Hence the map:

$$G_{\mathfrak{P}} \to \mathrm{Gal}(B/\mathfrak{P}, A/\mathfrak{p}), \ \sigma \mapsto \bar{\sigma}$$

is surjective and we have an exact sequence as claimed. In particular we get:

$$|G_{\mathfrak{P}}|/|I_{\mathfrak{P}}| = |\mathrm{Gal}(B/\mathfrak{P}, A/\mathfrak{p})| = f$$

and $|G_{\mathfrak{P}}| = ef$. Hence we get $|I_{\mathfrak{P}}| = e$ as claimed. □

Remark 7.5.

1. In the Galois situation we see that $\mathfrak{p}$ is unramified in L iff $I_{\mathfrak{P}} = 1$ for some (and hence any) $\mathfrak{P} \mid \mathfrak{p}$

2. In G we have:

   $$G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}$$

   and:

   $$I_{\sigma(\mathfrak{P})} = \sigma I_{\mathfrak{P}} \sigma^{-1}$$

   Thus the decomposition and inertia of the different prime ideals $\mathfrak{P} \mid \mathfrak{p}$ are conjugate subgroups in G.

3. for an *abelian* extension L/K the group $G_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ depend only on $\mathfrak{p}$!

Corollary 7.6. *In the Galois situation let $0 \neq \mathfrak{p}$ in A be a prime ideal and $\mathfrak{P}$ a prime ideal in B with $\mathfrak{P}mid\mathfrak{p}$. Let $I_{\mathfrak{P}} \subseteq G_{\mathfrak{P}} \subseteq G$ be the inertia and decomposition group of $\mathfrak{P}$ and let:*

$$T = L^{I_{\mathfrak{P}}}$$

be the so called inertia field and:

$$D = L^{G_{\mathfrak{P}}}$$

be the decomposition field of $\mathfrak{P}$. Let $B_T = B \cap T$ and $B_D = B \cap D$ be the integral closures of A in T respectively D. Set:

$$\mathfrak{P}_T = \mathfrak{P} \cap B_T \ , \ \mathfrak{P}_D = \mathfrak{P} \cap B_D$$

Let $e = e(\mathfrak{P} \mid \mathfrak{p})$, $f = f(\mathfrak{P} \mid \mathfrak{p})$ and r be the number of primes lying over $\mathfrak{p}$. Then we have the following picture:

		ramification index	inertia deg.	#prime factors	rel. deg. of ext.
B	$\mathfrak{P}$				
B_T	$\mathfrak{P}_T$	e	1	1	e
B_D	$\mathfrak{P}_D$	1	f	1	f
A	$\mathfrak{p}$	1	1	r	r

Thus $\mathfrak{p}$ decomposes in B_D with r different unramified prime ideals of inertia degree 1. Analogously for $\mathfrak{p}$ in B_T except that now all r prime ideals dividing $\mathfrak{p}$ have inertia degree f. Finally all ramification in the step from T to L.

Proof. We have seen:
$\mathfrak{P}$ is the only prime ideal over $\mathfrak{P}_D$ and $\mathfrak{P}_D = \mathfrak{P}^e$. ON the other hand: $\mathfrak{p} = \mathfrak{P}^e \dots$ and hence $\mathfrak{p} = \mathfrak{P}_D \dots$ i.e. $e(\mathfrak{P}_D \mid \mathfrak{p}) = 1$. Furthermore we showed that $A/\mathfrak{p} \simeq B/_D/\mathfrak{P}_D$ i.e.$f(\mathfrak{P}_D/\mathfrak{p}) = 1$
Finally:

$$\deg(D/K) = \deg(L/K)/\deg(L/D) = efr/|G_{\mathfrak{P}}| = efr/ef = r$$

Hence we have established the lower row in the picture. Next we see that:

$$(T : D) = (L : D)/(L : D) = |G_{\mathfrak{P}}|/|I_{\mathfrak{P}}| = ef/e = f$$

and:

$$(L : T) = |I_{\mathfrak{P}}| = e$$

This show the rightmost column in the picture:
We have shown that:

$$G_{\mathfrak{P}}/I_{\mathfrak{P}} \xrightarrow{\sim} \mathrm{Gal}(B/\mathfrak{P}, A/\mathfrak{p})$$

Apply this result to L/T instead of L/K. In that extension we have that the inertia group is equal to the decomposition group, since by definition the former is the entire Galois group. Hence we have:

$$\mathrm{Gal}(B/\mathfrak{P}, B_T/\mathfrak{P}_T) = 1$$

i.e.$f(\mathfrak{P} \mid \mathfrak{P}_T) = 1$. There is only one prime ideal over $\mathfrak{P}_T$ hence the degree formula gives:

$$(L : T) = e(\mathfrak{P} \mid \mathfrak{P}_T)$$

We saw above that $(L : T) = e$ and hence:

$$e(\mathfrak{P} \mid \mathfrak{P}_T) = e$$

Hence we've established the upper row in the picture. The formulas:

$$e = e(\mathfrak{P} \mid \mathfrak{p}) = e(\mathfrak{P} \mid \mathfrak{P}_T)e(\mathfrak{P}_T \mid \mathfrak{P}_D)e(\mathfrak{P}_D \mid \mathfrak{p})$$

and:

$$f = (\mathfrak{P} \mid \mathfrak{p}) = f(\mathfrak{P} \mid \mathfrak{P}_T)f(\mathfrak{P}_T \mid \mathfrak{P}_D)f(\mathfrak{P}_D \mid \mathfrak{p})$$

imply that:

$$e(\mathfrak{P}_t \mid \mathfrak{P}_D) = 1 \quad \text{and} \quad f(\mathfrak{P}_T \mid \mathfrak{P}_D) = f$$

thus we have established the middle row. □

We know turn our attention to the case where L/K is a Galois extension of number fields and $A = \mathcal{O}_K$ and so $B = \mathcal{O}_L$. Here all residue fields of non-zero prime ideals are finite and hence perfect. Let $\mathfrak{p} \neq 0$ be a prime ideal i $\mathcal{O}_K$ which is unramified in $\mathcal{O}_L$. Let $\mathfrak{P} \mid \mathfrak{p}$ be a prime ideal in $\mathcal{O}_L$ over $\mathfrak{p}$. Since:

$$1 = e = |I_{\mathfrak{P}}|$$

we have an isomorphism:

$$G_{\mathfrak{P}} \xrightarrow{\sim} \mathrm{GL}(\mathcal{O}_L/\mathfrak{P}, \mathcal{O}/\mathfrak{p})$$

We know from the Galois theory of finite fields that the group on the right is cyclic and generated by the Frobenius Fr_q for $q = |\mathcal{O}_K/\mathfrak{p}|$. Hence $G_{\mathfrak{P}}$ also cyclic of order f with a generator $\sigma = \sigma_{\mathfrak{P} \in G_{\mathfrak{P}}}$ which is uniquely determined by the condition $\bar{\sigma} = \mathrm{Fr}_q$ i.e. :

$$\sigma(x) \equiv x^q \bmod \mathfrak{P}, \ \forall x \in \mathcal{O}_L$$

We set:

$$(\mathfrak{P}, L/K) := \sigma_{\mathfrak{P}}$$

and call it the $\mathfrak{P}$-Frobenius. For $\tau \in G$ we have $\tau G_{\mathfrak{P}} \tau^{-1} = G_{\tau(\mathfrak{P})}$ and correspondingly:

$$\tau \circ (\mathfrak{P}, L/K) \circ \tau^{-1} = (\tau(\mathfrak{P}), L/K)$$

It follows that if the extension L/K is abelian the Frobenius $(\mathfrak{P}, L/K)$ depends only on $\mathfrak{p} \cap \mathcal{O}_K$. Think this case we denote it by $\mathfrak{p}, L/K \in G_{\mathfrak{p}} := G_{\mathfrak{P}}$

8 Decomposition of primes in cyclotomic fields

Lemma 8.1. *For a prime number p and $\nu \geq 1$ set $n = p^\nu$. Let ζ be a primitive p^ν-th root of unity. SEt $\pi = 1 - \zeta$. IN the ring of integers of $\mathbb{Q}(\zeta)$ the principle ideal:*

$$\mathfrak{P} = (\pi)$$

is a prime ideal over p of inertia degree $f = f(\mathfrak{P} \mid p) = 1$ We have:

$$(p) = \mathfrak{P}^e \quad \text{in} \quad \mathcal{O}_{\mathbb{Q}(\zeta)}$$

where $e = (\mathbb{Q}(\zeta) : \mathbb{Q}) = \varphi(p^\nu) = (p-1)p^{\nu-1}$. The basis $1, \zeta, \ldots, \zeta^{e-1}$ of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ has discriminant:

$$d(1, \zeta, \ldots, \zeta^{e-1}) = \pm p^s$$

where $s = p^{\nu-1}(p\nu - \nu - 1)$.

Proof. Did everything already. □

Theorem 8.2. *For $n \geq 1$ let ζ_n be a primitive n-th root of unity. Then we have:*

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$$

Moreover let $n = p_1^{\nu_1} \cdots p_t^{\nu_t}$ be the prime factor decomposition of n. Then there are $a_i \in \mathbb{Z}, a_i \geq 1$ such that:

$$d_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} = \pm d^{a_1}_{\mathbb{Q}(\zeta_{p_1^{\nu_1}})/\mathbb{Q}} \cdots d^{a_1}_{\mathbb{Q}(\zeta_{p_t^{\nu_t}})\mathbb{Q}}$$

Proof. First assume that $n = p^\nu, me = \varphi(p^\nu)$.Let ζ_{p^ν}. Using that:

$$d(1, \zeta, \ldots, \zeta^{e-1}) = \pm p^s$$

and Theorem 1.11 for $B = \mathcal{O}_{\mathbb{Q}(\zeta)}$ we get:

$$p^s B \subseteq \mathbb{Z}[\zeta] \subseteq B \tag{4}$$

For $\pi = 1 - \zeta$ the prime ideal $\mathfrak{P} = (\pi)$ has inertia index 1 by Lemma 7.1. Hence we have:

$$B/\pi B = \mathbb{Z}/p \quad \text{i.e.} \quad B = \mathbb{Z} + \pi B$$

and therefore:

$$\pi B + \mathbb{Z}[\zeta] = B$$

We get:

$$\pi^2 B + \pi \mathbb{Z}[\zeta] = \pi B$$

and together:

$$\pi^2 B + \mathbb{Z}[\zeta] = B$$

Arguing inductively we find:

$$\pi^k B + \mathbb{Z}[\zeta] = B \ \forall k \geq 1 \tag{5}$$

choose $k = e \cdot s$, then"

$$\pi^k B = (\pi^e B)^s = (pB)^s = p^s B \subseteq^{(1)} \mathbb{Z}\zeta$$

□

Using (2) we conclude $\mathbb{Z}[\zeta] = B$. For general n note the following fact from algebra:

Proposition 8.3. *For pairwise prime integers $n, m \geq 1$ let ζ_n and ζ_m be primitive roots of unity. Then we have:*

$$\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{mm})$$
$$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$$

Theorem 8.4. *Let L/K and L'/K be two Galois extensions of degrees n and n' with $L \cap L' = K$. Let $A \subseteq K$ be integrally closed with $\mathrm{Quot}(A) = K$ and let B and B' be the integral closures of A in L respectively L'. Let $w_1, \dots w_n$ respectively $w'_1, \dots, w_{n'}$ be the integral bases of B respectively B' over A with discriminants d, d'. If d, d' are coprime in the sense that $(d) + (d') = A$ i.e. $xd + x'd'$ for suitable $x, x' \in A$ then $w_i w'_j$ form an integral basis of the ring of integral elements (over A) in LL' with discriminant $d^{n'}(d')^n$*

Example 8.5. The ring of integrals of $\mathbb{Q}(\sqrt{5}, \sqrt{17})$ is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{17}}{2}]$.

Proof. By Galois theory the map:

$$\mathrm{Gal}(LL'/K) \xrightarrow{\sim} \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K)$$
$$\sigma \mapsto (\sigma|_L, \sigma|_{L'})$$

is an isomorphism and hence:

$$\deg(LL'/K) = \deg(L/K)\deg(L'/K) = nn'$$

The nn' products $w_i w'_j$ are K-linearly independent and hence a basis of LL' over K. Assume that $\alpha \in KL'$ is integral over A and write:

$$\alpha = \sum_{i,j} a_{ij} w_i w'_j \quad a_{ij} \in K$$

<u>Claim</u>: $a_{ij} \in K$

Indeed. Set $\beta_j = \sum_i a_{ij} w_i \in L$ and note that:

$$\mathrm{Gal}(LL'/K) = \{\sigma_k \sigma'_l\}_{k,l}$$

where:

$$\mathrm{Gal}(L/K) = \{\sigma_1, \dots \sigma_n\} \quad \mathrm{Gal}(L'/K) = \{\sigma'_1, \dots \sigma'_{n'}\}$$

Now let:

$$T = (\sigma'_l(w'_j))_{1 \leq l, j \leq n'}$$
$$a = (\sigma'_1(\alpha), \dots, \sigma'_{n'}(\alpha))^t$$
$$b = (\beta_1, \dots, \beta_{n'})^t$$

Then $\det T^2 = d'$ and $a = T(b)$. We have that:

$$(\det T)b = T^* T b = T^* a$$

where T^* denotes the adjunct matrix. Hence:

$$d'b = (\det T)T'a$$

has integral (over A) components i.e.:

$$d'\beta_j = \sum_i (d'a_{ij}) w_i \in B$$

hence:

$$a_{ij} = xda_{ij} = x'd'a_{ij} \in A$$

□

So the $w_i w'_j$ form an A-basis of the ring integral (over A) elements of LL'. the discriminant of this basis is $\det((\sigma_k(w_i))\sigma'_l(w'_j))^2_{(k,i),(l,j)}$ A calculation shows that this equals $d^{n'}d'^{n}$. We leave it as an exercise. □

Theorem 8.6. *Let $n \geq 1$ For a prime number P let $f_p \geq 1$ be minimal with:*

$$p^{f_p} \equiv 1 \bmod n'$$

where $n' = n/p^{\nu_p}$ and where p^{ν_P} is the highest power of p dividing n. Then:

$$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p\nu_p)} \quad \text{in} \quad \mathbb{Q}(\zeta_n)$$

where the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are pairwise different of inertia degree f_p. Moreover $r = \varphi(n')/f_p$

Remark 8.7.

1. The group $(\mathbb{Z}/n')^\times$ has order $\varphi(n')$¿ Hence an integers $f_p \geq 1$ as in the theorem exists sine p is prime to n'. Namely we have the f_p is the order of $\bar{p}$ mod n' in $(\mathbb{Z}/n')^\times$.
2. The theorem implies that p is ramified in $\mathbb{Q}(\zeta_n)$ iff $p \mid n$ and $\varpi(p^{\nu_p}) = (p-1)p^{\nu_p - 1} \geq 2$, i.e. if p is odd and $p \mid n$ or if $p = 2$ and $4 \mid n$.
3. Assume $p \nmid n$. Then p is unramified in $\mathbb{Q}(\zeta_n)$ and we have:

   $$(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

   with pairwise different prime ideal s $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ of inertia degree f_p each where $f_p \geq 1$ is minimal with:

   $$p^{f_p} \equiv 1 \bmod n$$

   We have $r = \varphi(n)/f_p$.

Proof. We can apply theorem 4.13 to all p since we know that $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ (conductor $f = (1)$). Let $\phi_n(x)$ be the minimal polynomial of ζ_n and $\bar{\phi}(X) \in \mathbb{F}_p[z]$ its reduction mod p. We have tho show that:

$$(*) \quad \bar{\phi_n}(X) = (\bar{P}_1 \cdots \bar{P}_r)^{\varphi(p^{\nu_p})} \in \mathbb{F}_p[X]$$

where the $\bar{P}_i(X)$ are pairwise different monic irreducible polynomials of degree f_p in $\mathbb{F}_p[X]$. We fist reduce to the case $p \nmid n$. Let $\{\xi_i\}$ respectively $\{\eta_j\}$ be the the sets of primitive n'-th respectively p^{ν_p}-th roots of unity (in an extension field of $\mathbb{Q}$). Then $\{\xi_i \eta_j\}$ is the set of primitive $n'p^{\nu_p} = n$-th roots of unity (!). WE find:

$$\phi_n(X) = \Pi_{i,j}(X - \eta_j \xi_i)$$

we have $\eta_j \equiv 1 \bmod \beta$ for all $\mathfrak{P} \mid p$ in $\mathbb{Q}\zeta_n$. Hence we get:

$$\phi_n(X) \equiv (\prod_i (X - \xi_i))^{\varphi(p^{\nu_p})} = (\varphi_{n'}(X))^{\varphi(p^{\nu_p})} \bmod \mathfrak{P}$$

Since all coefficients line in $\mathbb{Z}$ and $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$, we get:

$$\phi_n(X) \equiv \phi_{n'}(X)^{\varphi(p^{\nu_p})} \bmod p$$

i.e.:

$$\bar{\phi_n}(X) = \phi_{n'}(X)^{\varphi(p^{\nu_p})} \in \mathbb{F}_p[X]$$

By definition , $f_p \geq$ is minimal with $p^{f_p} \equiv 1 \bmod n'$. Hence it is sufficient to show $(*)$ or equivalently the theorem in the case $p \nmid n$. Then $p \nmid d_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ and hence p is unramified in the abelian extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. LET:

$$(p, \mathbb{Q}(\zeta_n)/\mathbb{Q}$$

be the Frobenius for p.

Lemma 8.8. *Under the isomorphism:*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n)^\times$$

we have:

$$(p, \mathbb{Q}(\zeta_n)/\mathbb{Q}) \mapsto p \bmod n$$

The decomposition group G_p of (p) in $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is cyclic of order $f(\mathfrak{P} \mid p)$ (any $\mathfrak{P}$ over p). with generator $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$. Hence:

$$\begin{aligned} f(\mathfrak{P} \mid p) &= \text{ order of } (p, \mathbb{Q}(\zeta_n)/\mathbb{Q}) \text{ in } \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ &=^{Lemma} \text{ order of } p \bmod n \text{ in } (\mathbb{Z}/n)^\times \\ &= f_p \text{ as in the theorem} \end{aligned}$$

□

Proof of Lemma. Choose a prime ideal $\mathfrak{P} \mid p$ in $\mathbb{Q}(\zeta_n)$. Let $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ correspond to $p \bmod n \in (\mathbb{Z}/n)^\times$. For all $x_i \in \mathbb{Z}$ we have:

$$\sigma_p(\sum_i x_i \zeta_n^i) = \sum_i x_i \zeta_n^{p_i} \equiv (\sum_i x_i \zeta_n^i)^p \bmod \mathfrak{P}$$

Thus σ_p satisfies the defining property of the Frobenius. □

Lemma 8.9. *Let $p \neq 2$ be a prime number. Then $\mathbb{Q}(\zeta_p)$ contains exactly one quadratic number field F. We have:*

$$F = \begin{cases} \mathbb{Q}(\sqrt{p}) \text{ if } p \equiv 1 \bmod 4 \\ \mathbb{Q}(\sqrt{-p}) \text{ if } p \equiv 3 \bmod 4 \end{cases}$$

equivalently:

$$F + \mathbb{Q}(\sqrt{p^*}) \quad \text{where } p^* = (-1)^{\frac{p-1}{2}} p$$

Proof. Let $K = \mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois with group $(\mathbb{Z}/p)^\times = \mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)$. Hence $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic of even order and therefore it contains exactly one subgroup of index 2, namely $(\mathbb{F}_p^\times)^2$. Hence K contains exactly one subfield F of degree 2 over $\mathbb{Q}$. Let ℓ be a prime number which ramifies in F. Then ℓ ramifies in K and hence $\ell = p$. Write $F = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z} \setminus 1$ squarefree. If $\not\equiv 1 \bmod 4$ then $d_{F/\mathbb{Q}} = 4d$ and hence 2 is ramified in F hence $p = 2$ which is a contradiction. Hence $d \equiv 1 \mod 4$ and $d_{F/\mathbb{Q}} = d$. Since d is squarefree and p is the only prime dividing d ($\equiv$ ramified in F) we get that $d = \pm p$. Since $d \equiv 1 \mod 4$ we find $d = p$ if $p \equiv 1 \mod 4$ and $d = -p$ if $p \equiv 3 \mod 4$. □

Proof of Quadratic Reciprocity. Fix odd prime numbers $p \neq \ell$. Set $K = \mathbb{Q}(\zeta_p)$. Let $(\ell, K/\mathbb{Q}) \in \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{F}_p^\times$ be the Frobenius automorphism of ℓ (note that ℓ is unramified in K, $K/\mathbb{Q}$ abelian). We know that:

$$\mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} \mathbb{F}_p^\times$$

$$(\ell, K/\mathbb{Q}) \mapsto \ell \mod p$$

This implies: [Stuff Missing]
Hence we have:

$$(\ell, F/\mathbb{Q}) = (\frac{\ell}{p})$$

under the identification:

$$\mathrm{Gal}(F/\mathbb{Q}) = \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 = \mu_2$$

On the other hand:

$$\begin{aligned}(\ell, F/\mathbb{Q}) = \mathrm{id} &\iff \text{ decomposition group of } \ \ell \text{ in } F \ \text{ is trivial} \\ &\iff \ell \ \text{ is decomposed in } \ F = \mathbb{Q}(\sqrt{p^*}) \\ &\iff p^* \ \text{ is a quadratic residue mod } \ \ell \\ &\iff \left(\frac{p^\times}{\ell}\right) = 1\end{aligned}$$

Analogously:

$$(\ell, F/\mathbb{Q}) \neq \mathrm{id} \iff (\frac{p^*}{\ell}) = -1$$

And hence putting these together:

$$\left(\frac{\ell}{p}\right)(\ell, F/\mathbb{Q}) = \left(\frac{p^*}{\ell}\right) = \left(\frac{-1}{\ell}\right)^{\frac{p-1}{2}}\left(\frac{p}{\ell}\right) = (-1)^{\frac{l-1}{2}\frac{p-1}{2}}\left(\frac{p}{\ell}\right)$$

□